Ithaca Renting Internet Service (IRIS)
Acceptable Use Policy

By using the Service, the Subscriber agrees to abide by, and require each user of the Service to abide by, the terms of this AUP and associated Terms of Service (TOS). Any user who does not agree to be bound by these terms must immediately cease use of the Service and notify the Ithaca Renting Company rental office to terminate the account.

Use: The Service is designed for personal use (residential use only) within a single apartment. Subscriber agrees that only Subscriber and Subscriber''s authorized guests in the same apartment will use the Service. Subscriber is responsible for any misuse of the Service that occurs through Subscriber''s account, whether by the subscriber or an authorized or unauthorized third-party. Subscriber will not use, or enable others to use, the Service to operate any type of business or commercial enterprise. Subscriber will not resell or redistribute, or enable others to resell or redistribute, access to the Service in any manner. Ithaca Renting Company reserves the right at its sole discretion to immediately suspend, terminate, or restrict use of the Service without notice if such use violates the AUP, is objectionable or unlawful, or interferes with IRIS’s systems, network, the Internet, or other subscribers' use of the Service.

Prohibited Activities: Any activity or use of the Service which violates system or network security or integrity are prohibited and may result in criminal and civil liability. Such violations include, without limitation, the following:

- 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.
- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner or network.
- Interference with Internet service to any user, host, or network, including but not limited to: mail bombing, flooding, or denial of service attacks.
- Forging the header of any transmitted information packet or email.
- Reselling or otherwise redistributing the Service.
- Disrupting, degrading or otherwise adversely affecting the network or computer equipment owned by other subscribers.
- Transmit unsolicited bulk or commercial messages commonly known as "spam."
- Assuming or assigning an IP address that was not allocated to the user. All users must use DHCP assigned by the Service to acquire an IP address.
- Hosting or use of any denial of service (DoS/DDoS) tool in any capacity
- Running any type of server on the system that is not consistent with personal use. This includes but is not limited to Bittorrent, FTP, IRC, SMTP, POP, HTTP, SOCS, SQUID, NTP, DNS or any multi-user forums.
- Distributing in any way information, software or other material obtained through the service or otherwise that is protected by copyright or other proprietary right, without obtaining any required permission of the owner.

Illegal or Fraudulent Use: The Service may be used only for lawful purposes. Subscriber will not use or allow others to use the service in any manner that is in violation of any applicable federal, state, local or international laws or regulations or to promote, engage in, or enable illegal activity or conduct that violates or infringes upon the rights of any person. Transmission or distribution of any material in violation of any applicable law or regulation is prohibited. This includes, without limitation, material protected by copyright, trademark, trade secret, or other intellectual property right used without proper authorization, and material that is obscene, illegal, defamatory, constitutes an illegal threat, or violates export control laws. Furthermore, use of the Service to impersonate a person or entity is not permitted.

Security/Abuse of Resources: User is solely responsible for the security of any device connected to the Service, including any data stored on that device. Users shall take all necessary steps to avoid actions that result in the abuse of a resource on their network. Examples of abuse of resources include without limitation: open news servers, open SMTP servers, unsecure wireless routers, and unsecure proxy servers. In the instance when the Subscriber is using a wireless router, any wireless network be secure and encrypted. Open, unencrypted wireless networks are strictly prohibited.

Viruses: Users must take appropriate action to prevent their systems from becoming infected with and/or distributing computer viruses such as but not limited to worms, "Trojan horses", denial of service attacks, and bots.

No Waiver: The failure to enforce any provision of this Policy at any given point in time shall not be construed as a waiver of any right to do so at any future time thereafter.

Should an issue arise, Subscriber is required to address the problem in a timely fashion. Failure to address an issue after notification will be considered a violation of this Acceptable Use Policy..