

TelecityGroup IP Services  
**Acceptable Use  
Policy**



# Document Control

Any updates or modifications to this document should be made in this copy of the document and summarised here. The Security Officer will review the amendments and sign them off before changes are made and an updated version of the document issued. This copy of the document will be kept as reference until the next revision.

Author/Reviewer	Revision Number	Date Changed	Reason	Reviewer
Carl Windsor	0.1	19-01-02	Initial Draft	
Carl Windsor	0.2	05-02-02	Release Candidate	
Carl Windsor	1.0	12-02-02	Final Release	
Carl Windsor	1.1	16-04-03	Legal review	Liz Hayman
Carl Windsor	1.2	01-08-03	Changes following UCE guidelines	Liz Hayman / James Tyler
Carl Windsor	1.3	03-01-05	Security Forum review	Security Forum
James Tyler	1.4	29-03-07	Revised following TeleCity / Redbus merger	James Tyler
Mariska van Beukering	1.5	22-11-07	Name change to TelecitGroup	Mariska van Beukering

This document has been reviewed and authorised  
by the TelecitGroup Security Forum

---

## Scope of the AUP

This AUP applies to all TelecityGroup IP Services customers including, but not limited to, IP Transit and IP Multihome. TelecityGroup IP Services customers who resell IP services are also responsible for ensuring that their own customers behave in a way consistent with the TelecityGroup IP Services AUP.

The AUP also applies to Internet traffic between TelecityGroup and networks with which TelecityGroup has a peering agreement. In other words, a peer network might have an AUP substantially different from the TelecityGroup AUP, but TelecityGroup will apply its own AUP to the traffic flowing across the peering connection.

It is the responsibility of the customer to keep up to date with the TelecityGroup Acceptable Use Policy the latest version of which must be adhered to regardless of contract initiation date. The current version can be found at <http://www.telecitygroup.com> 'AUP' link at the foot of the home page or can be obtained from your account manager or customer support contact.

## Reporting Internet misuse to TelecityGroup

Individuals and organisations who are the target of Internet abuse originating at a site connected to TelecityGroup (AS15830 or any other designated TelecityGroup network) are encouraged to report this to TelecityGroup via the abuse e-mail address [abuse@telecity.com](mailto:abuse@telecity.com). In all cases, the report should be substantiated with detailed time stamped logs and any other supporting documentation and the person or organisation reporting the misuse clearly identified with contact information including email address, telephone and fax numbers. TelecityGroup will be unable to take action as a result of reports which cannot be substantiated or reports sent to addresses other than [abuse@telecity.com](mailto:abuse@telecity.com).

If a site is found to be contravening the TelecityGroup IP Services AUP, we will take appropriate action, depending on the severity of the contravention.

## Legal responsibilities

TelecityGroup customers must, at all times, respect all relevant national and international legislation pertaining to the use of internet services including, but not limited to, access, content, storage of email addresses and associated email marketing campaigns.

## Unauthorised Use of Computer or Network resources

The unauthorised access or use by TelecityGroup IP Services customers of all types of computer or network resources connected to the Internet is expressly forbidden. This includes but is not limited to:

- Passive or non-invasive techniques such as security-hole scanning or bulk email bouncing.
- Unauthorised attempts by a user to gain access to any account or computer resource not belonging to that user (e.g. "cracking") by any method (e.g. physical or social).

- Unauthorised access, alteration, destruction or disruption, or any attempt thereof to TelecityGroup, TelecityGroup customers or other third party data and services.
- Obtaining or attempting to obtain service by any means or device with intent to avoid payment.
- Forging of any IP packet in order to "spoof" the source.
- Forging of any part of the header information in an e-mail or newsgroup posting to make it look as though it has come from a different source.
- Hosting or advertising of a site deliberately created to look like a third party web site for the purpose of fraud or disclosure of confidential information.

TelecityGroup reserves the right to disconnect a customer site that is involved in such activities without prior warning.

## Denial of Service attacks

TelecityGroup IP Services customers are forbidden to use techniques designed to cause damage to or to deny access by legitimate users of computers or network components connected to the Internet. This includes techniques such as SYN flood attacks, and giant packet Ping attacks etc. TelecityGroup reserves the right to disconnect a customer site that is the source of such activities without prior warning.

If the customer's network is used by a third party in an attack against someone (e.g. smurf amplifier, SQLSlammer, distributed denial of service attack), then TelecityGroup reserves the right to stop the traffic to the victim which includes disconnection of the customer without prior warning.

## Unsolicited Commercial Advertisements

TelecityGroup IP Services customers are prohibited from generating unsolicited commercial advertising in

- Personal email
- Email mailing lists
- Usenet discussion groups

Commercial advertising using these media is only permitted when the recipient has specifically and clearly indicated his desire to receive the material. TelecityGroup IP Services reserves the right to take technical steps to stop such misuse, which includes disconnection of the customer without prior warning.

## Bulk email and Usenet Spamming

TelecityGroup IP Services customers are prohibited from sending 'bulk' email (the same, unsolicited, email content to more than very few addresses), and from sending off-topic bulk postings to large numbers of Usenet groups ('spamming'). This rule holds whatever the content of the email or Usenet posting, even if it is not commercial in nature. TelecityGroup IP Services reserves the right to take technical steps to stop such misuse, which includes disconnection of the customer without prior notice.

## Guidelines for Permission-Based Email

While TelecityGroup prohibits the use of its systems or network to send unsolicited email (also described as SPAM, UCA, UCE, UBE) as described above, customers may send permission-based email marketing, subject to the guidelines provided herein. Permissionbased marketing is defined as electronic marketing that an end user agrees to receive. This is often referred to as 'opt-in' electronic marketing. All recipient information for such marketing conducted by TelecityGroup customers must be documented and catalogued by the customer. This information is to include date, time, originating IP and the location from which the email address or other recipient information was obtained. Additionally, a customer must at a minimum comply with the following guidelines, and any additional guidelines established by TelecityGroup from time to time in its sole discretion, to engage in permission-based email marketing without violating the AUP:

1. All commercial or bulk email originating from a TelecityGroup customer on the TelecityGroup network must have a working unsubscribe link. The customer must honour all requests to unsubscribe within 72 hours. Additionally, there must be text in the email stating that while all requests to unsubscribe are honoured, it may take up to 72 hours to process.
2. All commercial or bulk email originating from a TelecityGroup customer on the TelecityGroup network must clearly list the email address to which the email was originally sent (the intended recipient's email address) in the body of the message OR in the 'TO:' line of the email.
3. All TelecityGroup customers sending commercial or bulk email must have a working [abuse@domain.com](mailto:abuse@domain.com) address from EVERY domain associated with the email campaign. Additionally, the [abuse@](mailto:abuse@domain.com) address must be prominently posted on the front page of the associated web site. Customers must regularly answer any messages sent to the [abuse@](mailto:abuse@domain.com) address.
4. All TelecityGroup customers sending commercial or bulk email must register the [abuse@](mailto:abuse@domain.com) address for every domain associated with commercial email they send at <http://www.abuse.net/>.
5. All TelecityGroup customers sending commercial or bulk email must have a Privacy Policy/AUP posted for each domain associated with the email campaign.
6. All commercial or bulk email sent must include information about when and where the email address was obtained in the body of the email. For example:  
  
"You opted-in to receive this email promotion from our web site on 24/03/03."
7. All TelecityGroup customers sending commercial or bulk email must answer all complainants' requests for details regarding where the complainant "opted-in" to receive electronic marketing within 72 hours. This information must include the date, time, originating IP and the location from which the email address or other recipient information was obtained. Instructions on how to get this information must be

stated clearly in the body of the email. For example, a statement similar to the following must be present in the body of the email: "If you would like to learn more about how we received your email address, please contact us at [abuse@yourdomain.com](mailto:abuse@yourdomain.com)."

Requests for "opt-in" information must be responded to within 72 hours.

8. All TelecityGroup customers sending commercial or bulk email must be able to track and identify complainants.
9. If a TelecityGroup customer is using an affiliate program to send commercial or bulk email through the TelecityGroup network and the affiliate program becomes subject to repeated abuse by users, the customer must discontinue use of the affiliate program or be subject to immediate suspension or cancellation.
10. All customers of TelecityGroup are required to have up-to-date and valid contact information on file with their registrar for any domain hosted on the TelecityGroup network.
11. All customers must at all time comply with applicable data protection guidelines when contacting clients and when administering their email activities.
12. E-mails sent from a non-TelecityGroup IP address advertising sites hosted on a TelecityGroup network will be subject to the same acceptable use restrictions within this document.

TelecityGroup reserves the right to test portions of any customer's email list in response to complaints and request opt-in information from a random sample of that list at any time.

TelecityGroup reserves the right to determine in its sole discretion the validity of any customer's email list. Any list TelecityGroup determines in its sole discretion to be in violation of this AUP must be removed immediately or the customer will be subject to immediate suspension or termination. Repeated violations will result in permanent suspension.

TelecityGroup reserves the right to test and otherwise monitor customer's compliance with the above guidelines and requirements at any time during the customer's term of service at TelecityGroup.

If TelecityGroup determines in its sole discretion that the customer is not in strict compliance with the guidelines for permission-based e-mail marketing, then TelecityGroup may immediately suspend or terminate the customer's service.

TelecityGroup will not terminate a customer account without first requesting explanation and clarification of any reported e-mail AUP violation. However if such requests are ignored for more than 24 hours, services will be suspended until a response is received.

---

### **Illegal Material**

The content of any Internet traffic flow initiated by a TelecitGroup IP Services customer, whether flowing to or from a customer site, must not contravene local laws.

Transmission, distribution or storage of any material in violation of any applicable law of regulation is prohibited. This includes without limitation, material protected by copyright, trademark, trade secret, official secrets act or other intellectual property right used without proper authorisation, and material that is obscene, defamatory, constitutes and illegal threat or violates import or export control.

Even where local laws themselves do not explicitly prohibit a particular activity or Internet content, TelecitGroup itself does not permit its services to be used for activities which:

- Exploit minors
- Distribute copyrighted or licensed material
- Harass individuals or racial/ethnic groups

---

### **Security for customers' infrastructure within the TelecitGroup network**

TelecitGroup IP Services customers are responsible for the security of their assigned IP address range. Customers must take the appropriate action to ensure the security of their own networks and ensure that the network cannot be abused at any time or used to attack third parties.

If TelecitGroup becomes aware of a security threat to its own or another's network from a customer network, then steps will be taken to remove the threat, including disconnection of the customer's network without prior warning.

**TelecitGroup is a trading name of Telecit Group plc**