Acceptable Use Policies

1. Background

From time to time Luminet may impose reasonable rules and regulations regarding the use of its services. Such rules and regulations are called Acceptable Use Policies (AUPs) and are posted on the company's website. The AUPs are not exhaustive and Luminet reserves the right to modify the AUPs at any time, effective upon either the posting of the modified AUPs to the website or notification of the modified AUPs. By registering for and using the services, and thereby accepting the terms and conditions of the Master Services Agreement or its equivalent, you agree to abide by the AUPs as modified from time to time. Any violation of the AUPs may result in the suspension or termination of your account or such other action as Luminet deems appropriate. An unlisted activity may also be a violation of the AUPs if it is illegal, irresponsible, or disruptive use of the Internet. No credits will be issued for any interruption in service resulting from policy violations.

Violation of any AUP may result in the immediate termination or suspension of the services you receive from Luminet. You shall remain solely liable and responsible for your use of the services and any and all content that you display, upload, download or transmit through the use of the services. "content" includes, without limitation, your e-mail, web pages, personal home pages, and domain names. It is Luminet's policy to terminate repeat infringers. Luminet reserves the right to refuse service to anyone at any time.

2. Customer Security Responsibilities

The customer is solely responsible for any breaches of security affecting servers under customer control. If a customer's server is involved in an attack on another server or system, it will be shut down and an immediate investigation will be launched to determine the cause/source of the attack. In such event, the customer is responsible for the cost to rectify any damage done to the customer's server and any other requirement affected by the security breach. The labour used to rectify any such damage is categorised as emergency security breach recovery and is currently charged at **£175.00 per hour**. Enquiries regarding security matters may be directed to our Support team.

3. System & Network Security

Violations of system or network security are prohibited, and may result in criminal and civil liability. Luminet may investigate incidents involving such violations and may involve and will cooperate with law enforcement authorities if a criminal violation is suspected. Examples of system or network security violations include, without limitation, the following:

- Unauthorised 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 authorisation of the owner of such system or network.
- Unauthorised monitoring of data or traffic on any network or system without express authorisation of the owner of such system or network.
- Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks.

- Forging of any TCP-IP packet header or any part of the header information in an e-mail or a newsgroup posting.

Violators of the policy are responsible, without limitations, for the cost of labour to clean up and correct any damage done to the operation of the network and business operations supported by the network, and to respond to complaints incurred by Luminet. Such labour is categorised as emergency security breach recovery and is currently charged at £175.00 per hour required. Enquiries regarding security matters may be directed to the Support team. Luminet is concerned with the privacy of online communications and web sites. In general, the Internet is neither more nor less secure than other means of communication, including mail, facsimile, and voice telephone service, all of which can be intercepted and otherwise compromised. As a matter of prudence, however, Luminet urges its customers to assume that all of their online communications are secure. Luminet cannot take responsibility for the security of information transmitted over Luminet's facilities.

4. Password Protection

The customer is responsible for protecting customer's password and for any authorised or unauthorised use made of customer's password. The customer will not use or permit anyone to use Luminet's service to guess passwords or to access other systems or networks without authorisation. Luminet will fully cooperate with law enforcement authorities in the detection and prosecution of illegal activity.

5. Internet Etiquette

The customer is expected to be familiar with and to practice good Internet (N)etiquette The customer will comply with the rules appropriate to any network to which Luminet may provide access. The customer should not post, transmit, or permit Internet access to information the customer desires to keep confidential. The customer is not permitted to post any material that is illegal, libellous, tortuous, indecently depicts children or is likely to result in retaliation against Luminet by offended users. Luminet reserves the right to refuse or terminate service at any time for violation of this section. This includes advertising services or sites via IRC or USENET in clear violation of the policies of the IRC channel or USENET group.

6. Copyright Infringement / Software Piracy Policy

The Luminet network may only be used for lawful purposes. Transmission, distribution, or storage of any information, data or material in violation of any law is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secret, or other intellectual property rights.

Making unauthorised copies of software is a violation of the law, no matter how many copies you are making. If you copy, distribute or install the software in ways that the license does not allow, you are violating all law of copyright.

Luminet will cooperate fully with any civil and/or criminal litigation arising from the violation of this policy.

7. Responsible use of Network

Customers have a responsibility to use the Luminet network responsibly. This includes respecting the other customers of Luminet. Luminet reserves the right to suspend and or cancel service with any Customer who uses the Luminet network in such a way that adversely affects other Luminet customers. This includes but is not limited to:

- Attacking or attempting to gain unauthorised access to servers and services that belong to Luminet or its customers (i.e. computer hacking), and/or
- Participating in behaviour which result in reprisals that adversely effect the Luminet network or other customers' access to the Luminet network.

Luminet will react strongly to any use or attempted use of an Internet account or computer without the owner's authorisation. Such attempts include, but are not limited to, "Internet Scanning" ,password robbery, security hole scanning, port scanning, etc. Any unauthorised use of accounts or computers by a Luminet customer, whether or not the attacked account or computer belongs to Luminet, will result in severe action taken against the attacker. Possible actions include warnings, service suspension or cancellation, and civil or criminal legal action, depending on the seriousness of the attack. Any attempt to undermine or cause harm to a server, or customer, of Luminet is strictly prohibited.

Violations of this policy may be reported directly to the appropriate legislative / legal body.

8. Lawful Purpose

All services must be used for lawful purposes only. Transmission, storage, or presentation of any information, data or material in violation of any applicable law, regulation, or AUP is prohibited. This includes, but is not limited to: copyrighted material or material protected by trade secret and other statute or dissemination of harmful or fraudulent content.

Using any Luminet service or product for the purpose of participating in any activity dealing with subject matters that are prohibited under applicable law is prohibited.

Any conduct that constitutes harassment, fraud, stalking, abuse, or a violation of any government export restriction in connection with use of Luminet services or products is prohibited. Using the Luminet network to solicit the performance of any illegal activity is also prohibited, even if the activity itself is not performed. In addition, knowingly receiving or downloading a file that cannot be legally distributed, even without the act of distribution, is prohibited.

9. Child Pornography on the Internet

Luminet will cooperate fully with any criminal investigation into a Customer's violation of the Protection of Children Act 1978 concerning child pornography and the Protection of Children Act 199 and any equivalent legislation in force. Customers are ultimately responsible for the actions of their clients over the Luminet network, and will be liable for illegal material posted by their clients.

According to the Protection of Children Act, child pornography includes any type of visual presentation (eg. video , photographs, film) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or the dominant characteristic of which is the depiction, for a sexual purpose, of a an explicit sexual activity concerning a person under the age of eighteen years or any written material or visual

representation that advocates or counsels sexual activity with a person under the age of eighteen years.

Violations of the Protection of Children Act(s) may be reported to the relevant legislative body and /or law enforcement agency.

10. Unsolicited Commercial Email / Unsolicited Bulk Email

Unsolicited commercial email is defined by Luminet as any electronic communication (e-mail, ICQ, IRC, Instant Messenger, etc…) sent for purposes of distributing commercial information of any kind, soliciting the purchase or sale of products or services or soliciting any transfer of funds to a recipient who has not agreed to receive such communication.

Unsolicited bulk e-mail is defined by Luminet as any electronic communication (e-mail, ICQ, IRC, Instant Messenger, etc…) to multiple recipients who have not agreed to receive such communication.

Use of the Luminet network, servers or services to transmit any unsolicited commercial or unsolicited bulk-e-mail is expressly prohibited. Luminet also prohibits the sending of any fraudulent, malicious, harassing, false or misleading electronic communications, including, without limitation, chain letters, pyramid schemes, or e-mails with forged headers. Luminets customers are ultimately responsible for any violations of the AUP by their clients, and any violation of the AUP by a client of a Luminet customer shall be deemed a violation of the AUP by such Luminet customer.

Customers whose actions directly or indirectly result in Luminet IP space being listed in any of the various abuse databases may be subject to having the offending domain(s), server(s), or user(s) immediately removed from our network. In addition, if Luminet in its sole discretion determines that a customer is in violation of our AUP, Luminet may, at its sole discretion, restrict, suspend or terminate a customer's service. Luminet will, in most cases, attempt to contact a customer prior to suspension or termination of a server(s), but can not guarantee prior notification. Any server suspended or terminated for AUP violations will be reconnected only after the customer agrees to cease all activities that violate the Luminet AUP and pays all applicable reconnect fees and related charges. Any server suspended a second time for AUP violations WILL be immediately and permanently removed from our network.

Customers that Luminet determines in its sole discretion to be in violation of the Luminet AUP may be subject to additional fees or fines including, without limitation, any applicable reconnect fees.

11. Guidelines for Permission-Based Email

While Luminet prohibits the use of its systems or network to send unsolicited email as described above, customers may send permission-based email marketing, subject to the guidelines provided herein. Permission-based 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 Luminet 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 Luminet 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 Luminet customer on the Luminet 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 Luminet customer on the Luminet 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 Luminet customers sending commercial or bulk email must have a workingabuse@domain.com / .co.uk address from EVERY domain associated with the email campaign. Additionally, the abuse@ address must be prominently posted on the front page of the associated web site. Customers must regularly answer any messages sent to the abuse@ address.
4. All Luminet customers sending commercial or bulk email must have a Privacy Policy/AUP posted for each domain associated with the email campaign.
5. All commercial or bulk email sent must include information about 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 or from one of our partner sites."
6. All Luminet 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 atabuse@domain.com." Requests for "opt-in" information must be responded to within 72 hours.
7. All Luminet customers sending commercial or bulk email must be able to track and identify anonymous complainants. There are several software packages (such as RoboMail) that can help accomplish this.
8. If a Luminet customer is using an affiliate program to send commercial or bulk email through the Luminet 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.
9. All customers of Luminet are required to have up-to-date and valid contact information on file with their registrar for any domain hosted on the Luminet network.

12. Disclaimer

- Luminet 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.
- Luminet reserves the right to determine in its sole discretion the validity of any customer's email list. Any list Luminet 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.

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

13. IP Address Overlap

Luminet administers the network on which customer servers reside. The customer cannot use IP addresses which were not assigned to them by Luminet staff. Any server found using IPs which were not officially assigned will be suspended from network access until such time as the IP addresses overlap can be corrected.

14. IRC

Luminet allows the use of IRC inside the Luminet network as long as the use of IRC on a Luminet server does not violate any of the other terms of this AUP. As a policy, Luminet will not provide vanity IRC reverse DNS records. To enforce this policy Luminet does not turn the reverse address of IPs over to the customer. Authority over this information remains with Luminet.

15. Billing

The customer understands that the customer is responsible for paying for any network resources that are used to connect the customer's server to the Internet. The customer may request that the customer's server be disconnected from the Internet, but the customer will still be responsible for paying for any network resources used up to the point of suspension or cancellation.

16. Suspension

If Luminet in its sole discretion determines that a customer's server has become the source or target of any violation concerning the Luminet Acceptable Use Policy (AUP), Luminet reserves the right to suspend network access to that server. While Luminet will attempt to contact the customer before suspending network access to the customer's server(s), prior notification to the customer is not assured. In certain cases, Luminet will contact law enforcement and other agencies regarding these activities. Customers are responsible for all charges, as well as any fees relating to the investigation, suspension, administration and handling of their servers before, during and after the suspension period.

17. Cancellation

Luminet reserves the right to cancel service at any time, if inappropriate activity is detected. All accounts of the customer in question will be deactivated until an investigation is complete. Prior notification to the Customer is not assured. In extreme cases, law enforcement will be contacted regarding the activity. Any violation of policies which results in extra costs will be billed to the customer (i.e. transfer, space etc.).

18. Indemnification

Luminet wishes to emphasise that in signing the Master Services Agreement or its equivalent, customer indemnifies Luminet for any violation of the Master Services Agreement or its equivalent and any law or AUP that results in loss to Luminet or the bringing of any claim against Luminet by any third-party. This means that if Luminet is sued because of a customer or a customer of a customer's activity, the customer will pay any damages awarded against Luminet, plus costs and reasonable legal fees and costs.

19. Disclaimer of Responsibility

Luminet is under no duty to vet each customer's or user's activities to determine if a violation of the AUPs has occurred, nor does it assume any responsibility through its AUPs to monitor or police Internet-related activities. Luminet disclaims any responsibility for any such inappropriate use and any liability to any person or party for any other person's or party's violation of this policy.

All Sub-Networks, resellers and managed servers of Luminet must adhere to the above policies. Failure to follow any term or condition will be grounds for immediate Cancellation.

INDIRECT OR ATTEMPTED VIOLATIONS OF THE AUPs AND ACTUAL OR ATTEMPTED VIOLATIONS BY A THIRD PARTY ON YOUR BEHALF SHALL BE CONSIDERED VIOLATIONS OF THESE AUPs BY YOU.