ACCEPTABLE USE POLICY

1. **POLICY DESCRIPTION.** We have established this Acceptable Use Policy (this "Policy") in order to protect our services and networks and the Internet community as a whole, from improper or illegal activity. Pursuant to this Policy, we reserve the right to take certain preventative or corrective actions.

   As our customer, you and your users (employees and guests) may access the Internet through some of our services. The Internet provides a means for free and open discussion and dissemination of information. However, its openness makes it vulnerable to abuse. Because the information that you and your users create is carried over our networks and may reach a large number of persons, including both users and nonusers of our services, improper or illegal use of our services may negatively affect those other persons and may therefore harm our goodwill, business reputation, and operations. Pursuant to this Policy, we reserve the right to take certain preventative or corrective actions.

2. **REVISIONS AND CUSTOMER AGREEMENTS:** This Policy may be revised from time-to-time. Your use of our services, after changes to the Policy, will constitute your acceptance of any new or additional terms of this Policy that result from those changes. Your use of our services is subject to the terms and conditions of any agreements entered into between you and us. The Policy is incorporated into such agreements by reference.

3. **PROHIBITED ACTIVITIES.** You (and your users) violate this Policy and you violate your service agreement when you or your users engage in any of the following prohibited activities:

   A. **Spam and Facilitating Activities.** Sending unsolicited bulk and/or commercial messages over the Internet ("spam"), maintaining an open SMTP relay, or receiving responses to spam. Spam associated with our network is harmful because of its negative impact on consumer and industry attitudes toward us and because it can overload networks and disrupt service to our other customers and their users. When a complaint of spamming is received, we reserve the right to determine, in our sole discretion, whether or not an e-mail is spam based on whether or not the recipient list was derived from an "opt-in" e-mail list.

   B. **Robocalls.** The use of automated calling systems ("Robocalls") is prohibited, including the following associated activities: (i) transmission of automated voice calls without prior recipient consent; (ii) use of auto dialers, prerecorded messages, or artificial voice systems for unsolicited communications; (iii) any robocalling that violates federal, state, or local laws, including the Telephone Consumer Protection Act (TCPA) and Federal Trade Commission (FTC) guidelines; and (iv) circumventing caller ID authentication mechanisms or engaging in deceptive call practices (e.g. Spoofing). This prohibition does not apply to legally permitted automated calls, such as emergency alerts from schools or government agencies, healthcare appointment reminders, or other lawful notifications explicitly authorized by the recipient.

   C. **E-Mail Relay.** Any use of another person's electronic mail server to relay e-mail without express permission from the other person.

   D. **Forging of Headers.** Forging or misrepresenting message headers, whether in whole or in part, to mask the originator of the message or otherwise attempting to fraudulently conceal, forge, or otherwise falsify a sender's identity, or injecting false data into the Internet, for instance

in the form of bad routing information (including but not limited to the announcing of networks owned by someone else or reserved by the Internet Assigned Number Authority) or incorrect DNS information.

E. **Viruses, Worms, Trojan Horses, or Other Destructive Activities.** Distributing viruses, worms, Trojan horses, or engaging in pinging, flooding, mail bombing, or denial of service attacks, or distributing information facilitating the creation, distribution or engaging in any of the above. Destructive activities include any activity that has the effect of disrupting the use of or interfering with the ability of others to use effectively our networks or any connected networks, systems, services, or equipment.

F. **Illegal or Unauthorized Access to Other Computers or Networks.** Accessing illegally or without authorization computers, accounts, or networks belonging to another person; attempting to penetrate security measures of another person's system (often known as "hacking"), including any activity that might be used as a precursor to an attempted system penetration (e.g. port scan, stealth scan, or other information gathering activity); or attempting to intercept, redirect, or otherwise interfere with communications intended for others.

G. **Intellectual Property.** Engaging in any activity that infringes or misappropriates the intellectual property rights of others, including copyrights, trademarks, patents, service marks, and trade secrets. Software piracy is an example of such infringement. We are required by law to remove or block access to content upon receipt of a proper notice of copyright infringement. We may terminate the privileges of customers who commit repeat violations of copyright laws.

H. **Privacy and Other Personal Rights.** Engaging in activity that violates privacy, publicity, or other personal rights of others.

I. **Obscene Speech or Materials.** Using our networks to advertise, transmit, store, post, display, or otherwise make available child pornography or obscene speech or material. We are required by law to notify law enforcement agencies when we become aware of the presence of child pornography on or being transmitted through our networks.

J. **Defamatory or Abusive Language and Harassment.** Using our networks as a means to transmit or post defamatory, abusive, or threatening language, or to harass others, whether through language, frequency or size of messages.

K. **USENET Postings.** Posting to a USENET group material that is not in compliance with that group's charter and other policies, including cross-posting to unrelated news groups and posting of commercial messages (unless specifically invited by charter). Inappropriate postings also include those which have the effect of disrupting newsgroups with materials, postings, or activities that are (as determined by us in our sole discretion) frivolous, unlawful, obscene, threatening, abusive, libelous, hateful, excessive, or repetitious, unless such materials or activities are expressly allowed or encouraged under the newsgroup's name, FAQ, or charter.

L. **Export Control.** Unlawfully exporting encryption software to points outside the United States or otherwise violating export control laws or regulations.

M. **Other Illegal Activities.** Engaging in activities that are determined to be illegal, including advertising, transmitting, or otherwise making available Ponzi schemes, pyramid schemes, illegal gambling sites or services, fraudulently charging credit cards, and pirating software.

N. **Other Activities.** Engaging in activities, whether lawful or unlawful, that we reasonably determine to be harmful to our customers and their users, or to our operations, reputation, goodwill, or customer relations.

O. **Facilitating a Violation of this Policy.** Advertising, transmitting, or otherwise making available any software, program, product, or service that has the effect of violating or facilitating the violation of this Policy. Failure to cooperate effectively in preventing a violation of this Policy by one of your users is itself a violation of this Policy.

4. **NETWORK MANAGEMENT.** To preserve the integrity of our network, we implement reasonable network management practices to ensure that customers can effectively use the Internet. Activities that disrupt the use or interfere with the ability of others to effectively use the DQE network, system, service, or equipment by programs, scripts or commands including, but not limited to, Denial of Service Attacks (DDoS), SYN Floods, or similar activities shall be considered a violation of this Policy.

   You acknowledge that should you become the target of a DDoS or similar attack, DQE Communications ("DQE") reserves the right to block access to the IP address(es) being attacked until DQE can determine that the attack has ceased and is not likely to imminently return once service is restored. Should your server become the target of persistent, repeated attacks that require the intervention of a network administrator or attacks of sufficient scope to impact network performance and availability, DQE may choose to suspend or terminate services to maintain the quality of service for other customers on our network.

5. **CONSEQUENCES FOR VIOLATION OF THIS POLICY.** You are responsible for avoiding violations of this Policy, whether or not the violation is generated by you or a third party. We will not, as an ordinary practice, monitor the communications of our customers and their users to ensure that they comply with this Policy or applicable law. When we become aware of a violation of this Policy, however, we may take any action reasonably intended to stop the violation. Such actions may include, but are not limited to, removing information, shutting down a Website, implementing screening software designed to block offending transmissions, denying access to the Internet, and suspending or terminating our services. We may refuse to accept postings from newsgroups where we have knowledge that the content of the newsgroup postings is in violation of this Policy. We may take such actions against you, even though a violation may be generated by a third party rather than by you and even though the action may affect your other users. We may also take such actions directly against your user which is generating the violation, but we have no obligation to do so. We may require you to install and use any appropriate devices to prevent violations of this Policy, including devices designed to filter or terminate access to the services provided by us.

   We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy.

6. **COOPERATION.** We anticipate working closely and cooperatively with you to resolve violations of this Policy in most cases, as quickly as possible and with a minimum of disruption to operations and services. If you become aware of any violation of this Policy by any person, including your users, please notify us. We, in turn, will notify you in most cases of complaints received by us regarding incidents of alleged violation of this Policy by you or your users. (In cases where they

viability of our networks is threatened or which involve spamming, mail relaying, alteration of your source IP address information, denial of service attacks, illegal activities, harassment or copyright infringement, we reserve the right to suspend your service or your user's access to the service without notification") You should promptly investigate all such complaints and take all necessary actions to remedy and actual violation of this Policy. We may identify with the necessary information to contact you directly to resolve the complaint. You should identify a representative for the purposes of receiving such communications.