NETWORK MANAGEMENT POLICIES

Granite State Communications ("GSC") provides this Policy in order to disclose its network management practices in accordance with the FCC's Open Internet Rules. Information about GSC's other policies and practices are available at www.GraniteStateCommunications.com.

GSC manages its network to ensure that all of its customers experience a safe and secure broadband Internet environment that is fast, reliable and affordable. GSC wants its customers to indulge in all that the Internet has to offer, whether it is social networking, streaming videos and music, to communicating through email and videoconferencing.

GSC manages its network for a number of reasons, including optimization, as well as congestion- and security-protocol-management. But, very few of GSC's customers are impacted by the protocols and practices that GSC uses to manage its network.

GSC uses various tools and industry standard techniques to manage its network and deliver fast, secure and reliable Internet service. Such management tools and practices include the following:

Congestion Management

On GSC's network, all customers have access to all legal services, applications and content online and, in the event of congestion, most Internet activities will be unaffected. Some customers, however, may experience longer download or upload times, or slower surf speeds on the web when instances of congestion do occur on GSC's network.

Customers whose conduct abuses or threatens GSC's network or which violates the Company's Acceptable Use Policy or Internet service Terms and Conditions will be asked to stop any such use immediately. A failure to respond or to cease any such conduct could result in service suspension or termination.

Network Performance

GSC takes measurements of various components for network performance, analysis of the measurements to determine normal levels, and determination of appropriate threshold values to ensure required levels of performance for its network. GSC measures such components as network traffic load, latency, internal testing, and consumer speed tests to gauge network performance. GSC monitors the values of these components to determine the overall performance of the network. Customers using our FiberNet service can expect latency of less than 10ms on our network. Customers using our Quickstream DSL service can expect latency of less than 50ms on our network. Once customers reach the public Internet their experience is beyond the control of GSC and is subject to current traffic conditions.

Security Practices

GSC knows the importance of securing its network and customers from network threats and annoyances. The company promotes the security of its network and patrons by providing resources to its customers for identifying and reporting such threats as spam, viruses, firewall issues, and phishing schemes. GSC also deploys spam filters in order to divert spam from an online customer's email inbox while allowing the customer to control which emails are identified as spam.

As its normal practice, GSC does not block any protocols, content or traffic for purposes of network management except that the company may block or limit such traffic as spam, viruses, malware, or denial of service attacks to protect network integrity and the security of our customers. GSC also has a port filtering policy aimed at reducing the spread of computer-related viruses and protecting your computer from intruder access.

Except as may be provided elsewhere herein, GSC does not currently engage in any application-specific behaviors nor does it employ any device attachment rules for its network.

GSC limits email recipient lists to a maximum of 500 individual recipients via our webmail interface and 100 maximum individual recipients via a customers email program. Additionally, we restrict the use of non-GSC sendmail servers in an effort to stop the proliferation of spam from our network.

For the protection of the network and our customers, the following ports are blocked. The blocking of these ports protects against common viruses and worms, malicious intruders, and other security exploits.

Protocol	**Port**	**Transport**	**Inbound/Outbound**	**Reason**
SMB/Windows Shares	445	UDP/TCP	Both	Windows file sharing and other OS related services
FTP	21	TCP	Inbound	File Transfer Protocol servers can be exploited for illegal software hosting when configured improperly
NetBios	135-139	UDP/TCP	Both	NetBios services allow file sharing over networks. When improperly configured, they can expose critical system files or give full file system access (run, delete, copy) to any malicious intruder connected to the network.
RIP	520	UDP	Both	Vulnerable to malicious route updates which provides several attack possibilities.
SMTP	25	TCP	Both	Port 25 is an unsecured port on a computer Botnet spammers can take control of to send spam - often without the user ever knowing his/her computer has been compromised.
SSDP/UPnP	1900	UDP	Both	Network Protocol for denial of service abuse