NETWORK MANAGEMENT PRACT, the Company recognizes that, at times, network issues will arise and, during those times, the Company will undertake actions that are appropriate and tailored to achieving a legitimate network management purpose. The Company notes specifically, the following network management practices. *Blocking.* The Company does not block or otherwise prevent end user customer access to lawful content, applications, service, or non-harmful devices.

1. *Throttling.* Except where network congestion may occur, the Company strives to avoid any degradation or impairment of access to lawful Internet traffic on the basis of content, application, service, user, or use of a non-harmful device.
2. *Affiliated Prioritization.* The Company does not engage in any practice that directly or indirectly favors any of its affiliates' traffic over other traffic.
3. *Paid Prioritization.* The Company does not engage in any practice that directly or indirectly favors some traffic over other traffic in exchange for consideration, monetary or otherwise.
4. *Congestion Management.* The Company does not practice any congestion management.
5. *Applications-Specific Behavior.* The Company does not (i) block or rate-control specific protocols or protocol ports; (ii) modify protocol fields in ways not prescribed by the protocol standard; or (iii) otherwise inhibit or favor certain applications or classes of applications.
6. *Device Attachment Rules.* Provided that an attachment does not cause network harm, including by way of example, interference with the Company's network security measures, the Company does not restrict the types of devices that its end user customers may use and attach to the Company's network nor does it have any approval procedures for devices to connect to the Company's network.
7. *Security Measures.* In the event of Denial of Service (DoS), Distributed Denial of Service (DDoS) attack, spoofing or other malicious traffic, Decatur Telephone Company may implement inbound and outbound traffic filtering and/or blocking on specific source and destination IP addresses. These actions if implemented will be performed to ensure reliability and availability of the Smithville Telephone Company Inc. network. These actions will not be utilized for normal Internet applications and traffic. In the case of any suspicious or malicious network activity, notification and forensic information will be made available to the appropriate law enforcement and network security resources for investigation.