



## **Enterprise System & Services — Telecommunications Division**

### **Network Data Collection Standard**

It is the practice of Rutgers University to maintain access for its community to local, national and international sources of information and to provide an atmosphere that encourages the free exchange of ideas and sharing of information. Access to this environment and the University's information technology resources is a privilege and must be treated with the highest standard of ethics.

The university expects all members of the community to use computing and information technology resources in a responsible manner; respecting the public trust through which these resources have been provided, the rights and privacy of others, the integrity of facilities and controls, and all pertinent laws and university policies and standards.

Our customers have a reasonable expectation that Rutgers University Computing Services (OIT) will recognize and respect the privacy of the data that we transport across the university network on their behalf. It is a OIT policy to respect the privacy of its users and OIT will not monitor, edit, or disclose the contents of a user's communications unless required to do so by law or in the good faith belief that such action is necessary to respond to an operational problem or a security concern. OIT has responsibility for managing and maintaining equipment that makes forwarding decisions based on hardware address, Internet Protocol (IP) address, port number and size. OIT reserves the right to routinely collect gross characteristics (eg. source address, destination address, port numbers, size, etc.) from any university maintained network link. The payload portion of a datagram, that part which contains your information, would not be routinely captured or preserved. The primary purpose of collected data is to understand the traffic characteristics of the network, manage demand, plan for growth, and respond to network problems. OIT may also utilize this data to address identified or suspected security incidents. This data will be made available to authorized agents where required by law or where it is reasonable to believe that it is both unambiguous and necessary. This data is not available to resolve administrative disputes within, or between, business units.