Chief Operating Officer/Laura Williamson, Risk Management/Bill Hazelton, Facility Management/Sara Dorsett or Network Support/Brian Johnston or David O'Keefe).

12. Consistent Representation of Data

Fraud is a serious offense. Misrepresenting, obscuring, suppressing, or replacing a user's identity on an electronic communications system is forbidden. This is not just a violation of Glenmede's Security Policy, Rules & Practices. It is also a criminal offense.

13. Censorship of data

Sexual, ethnic, and racial harassment—including unwanted telephone calls, electronic mail, and internal mail—is strictly prohibited and is cause for disciplinary action including termination of the contract vendor relationship as well as potentially filing charges.

14. Communications Security

Third party questions about Glenmede's internal network or resources should be directed to Glenmede's Help Desk (ext 6689) or the Chief Technology Officer.

15. Network Connection

Prior IS approval is necessary for shared directory services and the use of devices for private networking (this includes the use of utilities like Laplink, PCanywhere, and PC direct connect).

No other ISP can be used to connect to the Internet from the Glenmede Network (i.e. AOL).

15. Encryption

No other encryption process or application may be used on a Glenmede resource that has not been authorized by Glenmede.

17. Dial-Up Communications

1. Do not publish Modem numbers.
2. Modem numbers will be changed at the discretion of IS Group.
3. Modems are not to be left in auto-answer mode without authorization from the Chief Technology Officer or the Security Officer.

18. Electronic mail

Users must not use an electronic mail account assigned to another individual to either send or receive messages.