Acceptable Use Policy – Version 2.3

Original document:
Computing and Electronic Communications at Duke University: Security & Privacy
(http://www.security.duke.edu/policies.html)

Revisions/Sign offs:
Version 2.3 – ITAC review (Conducted Feb 2009)
Version 2.2 - ISSC review and University Council review (Conducted Jan 2009)
Version 2.1 - ITAC Steering second document review (Conducted November 2008)
Version 2.0 - ITAC Steering first document review (Conducted September 2008)
Version 1.0 - ITAC statement on Security and privacy (Signed May 1997)

The purpose of this document is to establish and promote the ethical, legal, and secure use of computing and electronic communications for all members of Duke University and its affiliated entities, hereafter referred to as "Duke."

Comment: Addresses scope of coverage to include Health System and all other entities (Gap 1)

Duke cherishes freedom of expression, the diversity of values and perspectives inherent in an academic institution, the right to acknowledgment, and the value of privacy for all members of the Duke community. At the same time, Duke may find it necessary to access and disclose information from computer and network users' accounts to the extent required by law, to protect Duke's legal interests, to uphold contractual obligations or other applicable Duke policies, or to diagnose and correct technical problems. Under some circumstances, as a result of investigations, subpoena, lawsuits or threatened litigation, Duke may be required by law to provide electronic or other records or other information related to those records or relating to use of information resources ("information records"). Duke may in its reasonable discretion review information records, e.g., for the proper functioning of Duke or for internal investigations. For this reason, the ultimate privacy of messages, network transmissions and files cannot be ensured. In addition, system failures may lead to loss or exposure of data, so users should not assume that their messages and files are secure.

Comment: Addresses new e-discovery and legal procedure rules (Gap 2)

Comment: Addresses new e-discovery and legal procedure rules (Gap 2)

Comment: Addresses increased scrutiny of network transmissions under DMCA (copyright infringement rules) (Gap 4)

Comment: Recognizes general risk of data exposure (Gaps 2, 3, 6)

An account owner should not reveal a password to an IT support technician or any other individual, even though they may claim to work for the IT service (over the phone or in person). If, in the professional judgment of the user, it is necessary to share a password with an IT support technician or any other individual, the password must be changed as soon as possible thereafter. Once shared, a password is considered compromised and must be changed immediately.

Comment: Addresses Expanded Use of Duke credentials (Gap 5)

Neither Duke nor its agents restrict the content of material transported across its networks. While Duke does not position itself as a censor, it reserves the right to limit access to its networks or to remove material stored or posted on Duke computers when applicable Duke policies, contractual obligations, or state or federal laws are violated. In addition, users bear a personal responsibility to comply with all Duke policies, contractual obligations, and state and federal laws and regulations, including protecting the private information of others. Alleged violations will receive the same due process as any other alleged violation of Duke policy, contractual obligations, or state or federal laws.

Comment: Addresses HIPAA Security and Privacy regulation (Gap 3), NC Identity Theft protection Act (Gap6), PCI (Gap 7).

Comment: Addresses scope of coverage by deleting "academic" reference (Gap 1)