DEFINITIONS:

- **EVMS** includes
  - Eastern Virginia Medical School (EVMS)
  - Eastern Virginia Medical School Health Services (EVMSHS)
  - Eastern Virginia Medical School Pediatric Faculty Associates (EVMSPFA)

- **ITMT** refers to the appropriate member of the Information Technology Management Team comprised of the management representatives of:
  - The EVMSHS Data Processing Department
  - The EVMS Business and Financial Information Systems Center
  - The EVMS Network Information Center
  - The EVMS Data Base Center
  - The EVMS Communications Department
  - The EVMS Library Services

- **Information Services Department** refers to the technology department/personnel responsible for the related services.

GENERAL PRINCIPLES

Access to computer systems and networks owned or operated by Eastern Virginia Medical School imposes certain responsibilities and obligations and is granted subject to Medical School policies, and local, state, and federal laws. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment.

In making acceptable use of Information Technology resources you must:

- Use resources only for authorized purposes.
- Protect your user id and system from unauthorized use. You are responsible for all activities on your user id or that originates from your system.
- Access only information that is your own, that is publicly available, or to which you have been given authorized access.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Be considerate in your use of shared resources. Refrain from monopolizing systems, degrading services, or wasting connect time, disk space, printer paper, or other resources.

In making acceptable use of Information Technology resources you must NOT:

- Use another person's system, user id, password, files, or data without permission.
- Use computer programs to decode passwords or access control information.
- Attempt to circumvent or subvert system or network security measures.
  - Engage in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to Medical School data.
  - Use Medical School systems for commercial or partisan political purposes, such as using electronic mail to circulate advertising for products or for political candidates.
General Principles: Policy 1.10

- Use Medical School systems for sectarian religious purposes, i.e., those which do not embrace all religious beliefs, but espouse particular perspectives only.
- Make or use illegal copies of copyrighted software, store such copies on Medical School systems, or transmit them over Medical School networks.
- Waste computing resources or network resources, for example, by intentionally placing a program in an endless loop, printing excessive amounts of paper, or by sending chain letters or unsolicited mass mailings.
- Use the Medical School’s systems or networks for personal gain; for example, by selling access to your user id or to Medical School systems or networks, or by performing work for profit with Medical School resources in a manner not authorized by the Medical School.
- Engage in any other activity that does not comply with the General Principles presented above.

DISCIPLINARY PROCEDURES

Appropriate disciplinary action up to and including termination of employment will be taken when the provisions of this policy are violated. Refer to Human Resources Policies and Procedures – Disciplinary Action: Policy 4.50.