

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

| | | | |
|----------------------|---|-----------------|--|
| Chapter 5 | Information Management & Services | Effective: | June 2003 |
| Section 5.8 | Information Security | Revised: | September 2004 |
| Policy 5.8.17 | Information Security Training and Awareness Policy | Responsibility: | Vice President and Chief Information Officer |

INFORMATION SECURITY TRAINING AND AWARENESS POLICY

Policy

All users and data owners at the Health Science Center are required to receive adequate training on information security issues.

All new employees must attend the University's "New Employee Training" or the "New Faculty Training" which has an approved security awareness module as part of the training program. This training should be taken within thirty (30) days of being granted access to any University information resources.

All users must sign an acknowledgement stating they have read and understood the Health Science Center requirements regarding computer security policies and procedures. This acknowledgement form is provided at the above classes.

All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect Health Science Center information resources. In the case of contractors, consultants, or temporaries under contract, policy information is provided in accordance with University contract procedures.

All users must attend a computer security compliance session bi-annually which is part of the "General Compliance and Awareness Training" (GCAT).

All System Administrators (SysAdmin) and Technical Support Representatives (TSRs) are required to attend "Basic Information Security Training" which is formal classroom training designed to provide more technical information to the data custodians.

Additional operating system (OS) specific training is provided on an as available basis to provide SysAdmins with targeted security knowledge specific to the OS that they manage.

Training that targets a specific information security topic or organizational group (i.e. residents, researchers, or a particular department) can be arranged on request.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

| | | | |
|----------------------|---|-----------------|--|
| Chapter 5 | Information Management & Services | Effective: | June 2003 |
| Section 5.8 | Information Security | Revised: | September 2004 |
| Policy 5.8.17 | Information Security Training and Awareness Policy | Responsibility: | Vice President and Chief Information Officer |

Management and supervisor seminars are available which provide targeted information security material specific to regulatory, legal, and procedural issues affecting their operations.

Executive seminars designed to discuss strategic level information security issues, and answer questions and concerns about how information security impacts the missions of the University.

All available information security courses will be coordinated and posted through Technology Training in Information Management Client Support Services or Human Resources Training offices.

The Information Security Office will update policy and procedures periodically. The communication of these changes will occur through the TSR notification process using information security bulletins or will be posted on the information security website.

The University portal and the information security website are the primary locations to access the most up-to-date information regarding information security.

The Information Security Office is responsible for the overall management of the information security training program.
