National Institute of Standards and Technology (NIST) is a non-regulatory agency of the United States Department of Commerce's Technology Administration. The institute's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve quality of life. The Computer Security Act of 1987 assigned NIST the responsibility for the development and promulgation of cost-effective computer security standards and guidelines for the federal unclassified systems community. NIST's Computer Systems Laboratory (CSL) is also responsible for the development of standards and guidelines for federal computer systems including computer-related telecommunications systems.

The NIST special publication 800-14 explains the generally accepted principles and practices for securing information technology systems. The intrinsic expectations that must be met for securing a government agency or private corporation are termed as generally accepted system security principles. The principles address computer security from a very high-level viewpoint. The principles are to be used when developing computer security programs and policy and when creating new systems, practices or policies. These principles are derived from the Economic Co-operation and Development's (OECD) Guidelines for the Security of Information Systems.

The OECD Guidelines were developed in 1992 by a group of international experts to provide a foundation from which governments and the private sector, acting singly and in concert, could construct a framework for securing IT systems. The OECD guidelines include broad areas described below:

Accountability - The responsibilities and accountability of owners, providers and users of information systems and other parties...should be explicit.
Awareness - Owners, providers, users and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures...for the security of information systems.
Ethics - The Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interest of others are respected.
Multidisciplinary - Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints....
Proportionality - Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm....
Integration - Measures, practices and procedures for the security of information systems should be coordinated and integrated with each
other and other measures, practices and procedures of the organization so as to create a coherent system of security.
Timeliness - Public and private parties, at both national and international levels, should act in a timely coordinated manner to prevent and to respond to breaches of security of information systems.
Reassessment - The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.
Democracy - The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

Apart form the security principles, NIST 800-14 also describes security practices that are in general use. The practices guide organizations on the types of controls, objectives and procedures that comprise an effective IT security program. The practices show what should be done to enhance or measure an existing computer security program or to aid in the development of a new program.

The NIST 800-14 describes eight principles and fourteen practices. Each of the principles applies to each of the practices. In some cases, practices are derived from one or more principles; in other cases practices are constrained by principles. For example, the Risk Management Practice is directly derived from the Cost-Effectiveness Principle. However, the Comprehensive and Reassessment Principles place constraints on the Risk Management Practice.

The different practices that are listed by 800-14 can be summarized as follows:

Policy: • Program Policy • Issue-Specific Policy • system-Specific Policy	**Awareness and Training**
Program Management: • Central Security Program • System-level Program	**Security Considerations in Computer Support and Operations**
Risk Management: • Risk Assessment • Risk Mitigation • Uncertainty Analysis	**Physical and Environmental Security**
Life Cycle Planning: • Security Planning • Initiation Phase • Development / Acquisition Phase • Implementation Phase • Operation / Maintenance Phase • Disposal Phase	**Identification and Authentication:** • Identification • Authentication • Passwords • Advanced Authentication
Personnel / User Issues: • Staffing • User Administration	**Logical Access Control**
Preparing for Contingencies and Disasters: • Business Plan • Identify Resources • Develop Scenarios • Develop Strategies • Test and Revise Plan	**Audit Trails:** • Contents of Audit Trail Records • Audit Trail Security • Audit Trail Reviews • Keystroke Monitoring
Computer Security Incident Handling: • Uses of a Capability • Characteristics	**Cryptography**

References:

http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
http://www.nist.gov
http://en.wikipedia.org/wiki/NIST
http://csrc.nist.gov/publications/nistbul/csl91-02.txt