ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

ENGINEERING PRINCIPLES FOR INFORMATION TECHNOLOGY SECURITY

By Gary Stoneburner, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

In June 2001, ITL released NIST Special Publication (SP) 800-27, *Engineering Principles for Information Technology Security (EP-ITS),* by Gary Stoneburner, Clark Hayden, and Alexis Feringa. This bulletin presents an overview of the document.

> **Principle n.** — A rule or standard, especially of good behavior.
>
> *American Heritage Dictionary*

Engineering Principles for Information Technology (IT) Security (EP-ITS) provides a list of system-level security principles to be considered in the design, development, and operation of an information system. The EP-ITS principles can be used by:

- **Users** when developing and evaluating functional requirements or when operating information systems within their organizations.
- **System Engineers and Architects** when designing, implementing, or modifying an information system.
- **IT Specialists** during all phases of the system life-cycle.
- **Program Managers and Information System Security Officers (ISSO)** to ensure adequate security measures have been considered for all phases of the system life-cycle.

Background

Private businesses and government agencies, both foreign and domestic, are becoming increasingly reliant on information technology to fulfill many basic functions. Businesses are making changes simply to remain competitive in the changing global marketplace. Likewise, government agencies are seeking to provide better service to their citizens.

Seeking to support and guide these automation efforts, several private and public organizations have developed a number of explicit and implicit information system security principles. These security principles, in turn, have the potential to become an extensive canon for users, designers, and engineers to consider in designing information system security programs.

EP-ITS seeks to compile and present many of these security principles into one, easy-to-use document for those concerned with information system security. In contrast to other organization-level efforts, the principles presented in EP-ITS are structured around a system-level, engineering approach.

Security Principles

These principles provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities can be constructed.

While the primary focus is the implementation of technical controls, these principles also highlight the fact that, to be effective, a system security design should also consider non-technical issues, such as policy, operational procedures, and user education.

The principles described here do not apply to all systems at all times. Yet each principle should be carefully considered throughout the life-cycle of every system. Moreover, because of the constantly changing information system security environment, the principles identified are not considered to be an inclusive list. Instead, as technology improves and security techniques are refined, additions, deletions, and refinement of these security principles will be required.

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since December 1999

Table 1: EP-ITS Engineering Principles

Principle 1.	Establish a sound security policy as the "foundation" for design.
Principle 2.	Treat security as an integral part of the overall system design.
Principle 3.	Clearly delineate the physical and logical security boundaries governed by associated security policies.
Principle 4.	Reduce risk to an acceptable level.
Principle 5.	Assume that external systems are insecure.
Principle 6.	Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
Principle 7.	Implement layered security (Ensure no single point of vulnerability.).
Principle 8.	Implement tailored system security measures to meet organizational security goals.
Principle 9.	Strive for simplicity.
Principle 10.	Design and operate an IT system to limit vulnerability and to be resilient in response.
Principle 11.	Minimize the system elements to be trusted.
Principle 12.	Implement security through a combination of measures distributed physically and logically.
Principle 13.	Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
Principle 14.	Limit or contain vulnerabilities.
Principle 15.	Formulate security measures to address multiple overlapping information domains.
Principle 16.	Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
Principle 17.	Use boundary mechanisms to separate computing systems and network infrastructures.
Principle 18.	Where possible, base security on open standards for portability and interoperability.
Principle 19.	Use common language in developing security requirements.
Principle 20.	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
Principle 21.	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
Principle 22.	Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
Principle 23.	Use unique identities to ensure accountability.
Principle 24.	Implement least privilege.
Principle 25.	Do not implement unnecessary security mechanisms.
Principle 26.	Protect information while being processed, in transit, and in storage.
Principle 27.	Strive for operational ease of use.
Principle 28.	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
Principle 29.	Consider custom products to achieve adequate security.
Principle 30.	Ensure proper security in the shutdown or disposal of a system.
Principle 31.	Protect against all likely classes of "attacks."
Principle 32.	Identify and prevent common errors and vulnerabilities.
Principle 33.	Ensure that developers are trained in how to develop secure software.

Principle Applicability to System Life-Cycle Phase

The five life-cycle planning phases used are defined in NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*:

- Initiation Phase
- Development/Acquisition Phase
- Implementation Phase
- Operation/Maintenance Phase
- Disposal Phase.

In an effort to associate each principle with the relevant life-cycle planning phase(s), Table 2 summarizes the relationship between the 33 principles and the life-cycle phases to which they apply. The table identifies each life-cycle phase, and "check marks" are used to indicate if the principle should be considered or applied during the specified phase. One check "✔" signifies the principle can be used to support the life-cycle phase, and two checks "✔✔" signifies the principle is key to successful completion of the life-cycle phase.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our web site is http://www.itl.nist.gov/.

Table 2: Principle versus Life-Cycle Phases

	Life-Cycle Applicability				
Principle	**Initiation**	**Devel/Acquis**	**Implement**	**Oper/Maint**	**Disposal**
1	✔✔	✔	✔	✔	✔
2	✔✔	✔✔	✔✔	✔✔	✔
3	✔✔	✔✔	✔	✔	
4	✔✔	✔✔	✔✔	✔✔	✔✔
5	✔✔	✔✔	✔✔	✔✔	✔
6	✔✔	✔✔		✔✔	
7	✔	✔✔	✔	✔✔	✔
8	✔	✔✔	✔	✔✔	✔
9	✔	✔✔	✔	✔✔	
10	✔	✔✔		✔✔	
11	✔	✔✔	✔	✔✔	
12		✔✔	✔	✔	✔
13	✔	✔✔	✔	✔✔	✔
14		✔✔	✔	✔	
15	✔	✔✔	✔	✔	
16	✔	✔✔	✔	✔	
17		✔✔	✔	✔✔	
18	✔	✔✔	✔		
19	✔✔	✔✔		✔✔	
20	✔	✔✔	✔✔	✔	
21		✔✔	✔	✔✔	
22	✔	✔	✔	✔✔	
23	✔	✔	✔	✔✔	
24	✔	✔	✔	✔✔	
25	✔	✔✔	✔✔	✔	✔
26	✔	✔✔	✔	✔✔	✔
27	✔	✔✔	✔	✔✔	
28	✔	✔	✔	✔✔	
29	✔	✔✔	✔	✔	
30		✔		✔	✔✔
31	✔	✔✔	✔✔	✔	✔
32		✔✔	✔✔		
33	✔✔	✔✔	✔		

Summary

Now, more than ever, IT security is a critical element throughout the system life-cycle. Security must be incorporated and addressed from the initial planning and design phases to disposal of the system. Without proper attention to security, an organization's information technology can become a source of significant mission risks. With careful planning from the earliest stages, however, security becomes an enabler, supporting and helping to achieve the organization's mission.

As security awareness becomes a way of life within an organization, people at all levels, and roles in the system life-cycle, should have access to easily understood guidance. From users to system administrators and program managers, everyone should have a basic understanding of the security principles governing the system they are using, maintaining, or designing and developing.

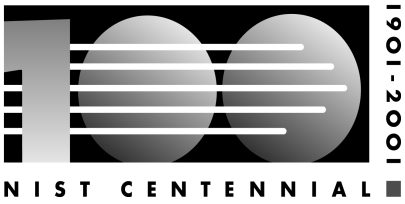
EP-ITS provides a starting point. The principles it contains are derived from a number of national and international documents, as well as from the experience of the scientists at NIST. It is hoped that these principles will contribute to improved IT security in any organization.

The complete NIST SP 800-27 document is available at http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.



U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900

Official Business
Penalty for Private Use $300
Address Service Requested

PRSRT STD
POSTAGE & FEES PAID
NIST
PERMIT NUMBER G195