HELLENIC REPUBLIC

MINISTRY OF INTERNAL AFFAIRS,
PUBLIC ADMINISTRATION & DECENTRALIZATION

GENERAL SECRETARIAT OF PUBLIC ADMINISTRATION

INFORMATION TECHNOLOGY DEVELOPMENT SERVICE

DEPARTMENT OF INFRASTRUCTURE

TO: All Ministries,
Self-contained General Secretariats,
Regional General Secretariats and
Prefectural Administrations
a) Administrative departments
b) Information Technology Departments

ATT: Ministers Offices
Minister of State Offices
General Secretaries of Ministries
General Secretaries of Self-contained General Secretariats
General Secretaries of Regions
Prefects

Athens, 13 / 02 / 1998
File Number.
YAP/F.06.11/3633

SUBJECT: "Security of Public Sector's Information Systems"

1. In recent years, the operation of Public Sector's Operators not only in our country but internationally also, is based on the use of information systems. Vast amounts of critical data, which are related to particularly critical state operations, are stored electronically, subjected to all the necessary processes and distributed by means of information systems.

The most important reasons, which render the issue of Public Sectors information systems security of high importance, are:
a) The expansion of information systems usage in the Public Sector.
b) The accumulation and electronic storing in them of large volumes of data, which are critical for the operator's functionality.
c) The need for protecting the secrecy of these data.
d) The need for high availability of the aforementioned data, which for many operators are prerequisite for their fundamental operation, even for their survival.
e) The need for reassurance of the integrity and reliability of the aforementioned data.
f) The continuing increase of complexity of the new information and telecommunications technology used.
g) The importance and magnitude of the realizing investments for creating, maintenance and utilization of information systems in the Public Sector's operators.
h) The rising of electronic crime observed.

2. A critical factor for information systems security of the Public Sectors operators is ***secrecy protection*** of the data, which are electronically stored in them.

Recent developments provide for capabilities of storing large volumes of data in small sized means of electronic storage, resulting in facilitating their leaking. This problem is worsening by the continuously expanding network connection of computers of different sizes, my means of local and wide range networks. Much of these data are particularly critical and sensitive thus, their leak, besides the competent and authorized for usage employees, can cause important moral and material damages in numerous citizens and corporations, while at the same time can provide in other citizens and corporations with unallowable moral and material benefits.

The physical and electronic control in accessing of Public Sector operators' information systems, can contribute in high degree in the protection of secrecy of the aforementioned electronically observed data.

3. An additional important factor of Public Sector operators' information systems security is the reassurance of ***integrity*** of these data, which are kept electronically in them.

The term integrity stands for the protection of these data by mistaken (accidental or in purpose) modifications and deletions that are reducing their reliability and can cause erroneous administrative actions and decisions damaging citizens and corporations.

Proper organization of information systems operation and utilization and rational development, testing and documentation of the software utilities used, can contribute significant in the reassurance of integrity, pertinence and reliability of the aforementioned data in conjunction always with physically and electronically controlled access in them.

4. Finally, another significant factor for public Sector's information systems security is reassuring their ***availability***.

In many Public Sectors' operators, non-availability of information systems when needed, either due to physical damages (e.g. fire, flooding, sabotage, etc.,) or due to various damages (e.g. power cut, damages to various hardware components, etc.,) can cause serious operational problems with especially unpleasant consequences.

Proper positioning, room configuration and equipping of Data processing centers with the necessary infrastructure, in conjunction with suitable policies for:

a) software and hardware maintenance;
b) auxiliary equipment, and
c) spare copies of electronic data,

Can contribute in reassuring the desirable high level of availability and preventing all the relevant operation problems.

5. The actions that have to be made for keeping the security of an operators information system are in general and on high degree depending on its features and distinctiveness. According to international experience, a complete security program of information systems is essential to comprise actions in five (5) levels:

a) Legislation
b) Internal Regulation
c) Physical Protection
d) Organization and Processes

e) Electronic protection (of software and hardware)

Some practical steps that every Public Sector's operator has to made for maintaining the security of information systems are:

- Detection of fundamental dangers and problems regarding information systems security considering all of their distinctiveness, and classification in levels of priority.
- Definition of all the necessary actions that must be taken under the five aforementioned levels, for treating the dangers stated above and security problems (mainly those with high priority).
- Establishing a time table for accomplishing these actions
- Providence that in all information systems studies and projects which the operator is to realize, special attention must be paid on issues concerning their security.

For more effective coordination of Public Sectors operators on issues concerning information systems security, we request the following:

a) All Information Technology Departments must return filled the attached questionnaire to Information Technology Development Service on March 20 1998 the latest, and
b) All Administrative Departments should notify their supervising operators the soonest possible.

6. Discriminations regarding the contents of this regulation are provided by Mr. Alexandros Levedides, Supervisor of Department of infrastructure and Mr. Euripides Loukis, Special Scientist (phone 3393254, 3393276).

Minister

Alexandros Papadopoulos