STATISTICAL DATA PROTECTION IN THE STATE STATISTICAL OFFICE OF THE REPUBLIC OF MACEDONIA

Contributed paper

Submitted by the State Statistical Office, The former Yugoslav Republic of Macedonia [1]

I.   INTRODUCTION

1.   The data protection project has been carried out within the framework of the Strategy for development of the statistical information system of the State Statistical Office. This project elaborates the data access rights and the use of data in the statistical information system. In order to increase data consistency and data confidentiality, in the information system user rights are precisely defined, and user groups with appropriate privileges are created.

2.   User groups in the statistical information system in The former Yugoslav Republic of Macedonia, based on the level of privileges are the following:

- Administrators: users with highest possible privileges in the system;
- Programmers: users with privileges to use system resources needed for application development and databases;
- System operators: users limited to operator functions (system shut down, printers, magnetic tapes);
- Standard users of the system: users with the lowest privileges, limited to strictly pre-defined system functions and resources.

3.   The State Statistical Office is not using special software for statistical disclosure control, but in its future activities it is planned to study and implement special software for this purpose.

II.   DEFINITION OF USER NAMES AND PASSWORDS

4.   While defining and registering a new user in the system, in addition to assigning a user name for entering the system, each user is given a password corresponding with its user name. While defining the user name and password the following criteria are taken into consideration: user name to identify the person or his/her post. The passwords are selected in a way to remain confidential and personalized to the user.

5.   The passwords should be created as randomly as possible in order to avoid intentional misuse of the access right with the use of someone else's password while associating it with the name of the user, date of birth, child or spouse name, address etc.

---

[1] Prepared by Slobodan Karajovanovic and Valentina Dzukevska Stefanovska.

6.   Basic rules for creating the password are:

- password should not be trivial;
- minimum eight characters;
- combination of letters and digits (minimum 2 digits);
- not to repeat some previously defined password;
- will be changed after a certain period.

7.   It is also important to define the schedule for password change. The duration of a password should be one month for users with limited privileges (standard users, programmers and operators). For users with administrative privileges the duration of the password should be one week due to the importance of thesepasswords for data security. After this period,the user is obliged to change the password. The administrator's duty is to change his/her password even sooner if he/she suspects that another user might know the password.

8.   It is very important that users that have been logged into the system log out whenever they are not present on their terminal/PC in order to avoid use of the system by someone else within the same work session.

9.   Use of the same user name by more than one user is not recommended because of shared responsibility in case of a problem and accidental or deliberate destruction of data on the system. Opening new user names is done by the system administrator.

III.   TYPE OF USERS AND THEIR PRIVILEGES

10.   In the system there are several different users according to their privileges:

- Administrators
- Programmers
- System operators
- Standard Users

Administrators

11.   Administrators are users with the greatest privileges in the system. They are responsible for the proper functioning of the system, for availability of the resources, for management of the subsystems, etc. According to the duties and responsibilities, there are several types of administrators:

- *System administrator* has all the rights and authorization for managing the whole system and all the subsystems. In the hierarchy of the administrators and generally in all users the system administrator takes the highest chair according to the user rights who is responsible for:
- definition of new system users;
- regular system functionality;
- providing adequate system resources;
- control of the processes;
- solving eventual problems;
- creating system archive;
- reconstruction of the system after eventual failure;
- recovery of damaged data;
- management of different system components.

- *Database administrator* is responsible for managing the subsystem for database management and is in charge of:

- maintenance of consistency of databases;
- definition of users/privileges for database access;

- archiving databases;
- solving eventual problems with the databases;
- recovery of the subsystem for database management;
- recovery of the databases.

- *ADSM Administrator* has the responsibility and authorization to manage the subsystem for data storage management – ADMS and must ensure the:

- correct functioning of the ADMS subsystem;
- definition of ADMS users/clients;
- configuration of the parameters of the ADMS subsystem;
- solving eventual problems with the subsystem;
- recovery of the ADMS subsystem;
- recovery of data.

- *Network administrator* is responsible for monitoring, configuration and management of the LAN and WAN as well as problem solving in this segment of the IT system.

Programmers

12.   Programmers are users that have privileges to use the system resources for application development and access to databases. They have the responsibility to create and update databases, to create different object of the system, to create and modify different programs/applications and other activities connected with the application development.

Operators

13.   Operators are who are restricted to operating functions of the system. They are in charge of management of network printers, transferring and coping databases, working with different system units (magnet tapes,...) and simple monitoring of the system activity.

Standard Users

14.   Standard users are users with the fewest responsibilities that are restricted only to using the exact determined subset of functions and resources of the system. They can access restricted subset databases (depending on which data they need for everyday work). They can use applications for data entry, or for generating reports, and they can archive their data/files on predefined storage place. Most of them are users of PCs that only have a need to be connected as clients on the servers of the systems.

15.   This way of organizing IT users provides overall confidentiality and security of data. Only by respecting the defined rules, can complete consistency and availability of data form the State Statistical Office be provided.