The Information Security Policy of the Statistical Office of the Republic of Slovenia

History of changes:

Version	Date	Document number
1	21 September 2011	007-47/2011/1
2	24 April 2015	007-47/2011/26
3	29 November 2017	007-47/2017/1
4	18 October 2018	007-47/2017/20

CONTENTS

On the basis of Paragraph 2 of Article 42 of the National Statistics Act (OJ RS, No. 45/95 and 9/01) and in line with Paragraph 1 of Article 80 of the Decree on Administrative Operations (OJ RS, No. 20/05, 106/05, 30/06, 86/06, 32/07, 63/07, 115/07, 31/08, 35/09, 58/10, 101/10 and 81/13) the Director-General of the Statistical Office of the Republic of Slovenia issued the following

Information Security Policy of the Statistical Office of the Republic of Slovenia

1. THE AIM AND OBJECTIVES OF THE INFORMATION SECURITY POLICY

The aim of the Information Security Policy is to set up the comprehensive data and information security management system at the Statistical Office of the Republic of Slovenia (SURS), with the objective to provide for the operation of SURS in line with the legal and business requirements.

The information and data security covers a set of technical and organisational measures, the aim of which is to safeguard and ensure integrity, availability, applicability, accessibility and confidentiality of information and data processed and prepared by SURS and to provide the continuity of SURS's operation. Management of information security must be in line with other organisational processes. The information security measures are carried out for the protection against a wide range of threats or to diminish the damages that would arise should these threats be carried out. In order to successfully attain this objective, adequate awareness of the importance of security and the culture on the information security must be set up and maintained by all SURS's employees; they must be familiar with and act in line with the adequate legislation and all the internal rules on information security.

The information security measures are adjusted to the organisational, business and strategic objectives of SURS and the legislation in force. The information security management system is the basis for diminishing the information risks, thereby ensuring successful implementation of SURS's tasks and business activities.

2. THE SCOPE AND BASIC PRINCIPLES OF INFORMATION SECURITY

2.1 Scope

This information security policy is the fundamental document on the management of information and data security at SURS. The policy comprises SURS's general guidelines and principles of information security and it refers to all the information assets used by SURS. Together with the rules, instructions and other documents adopted within its framework (hereinafter: information security policy) it is the formal framework of the information security management system at SURS.

This policy is addressed to SURS's employees, staff employed under contract, other collaborators (i.e. outsourcing) and all other persons with access to SURS's information assets (hereinafter: users). All these are to respect this policy and other rules on information security, and also all the organisational and technical measures concerning information security at SURS.

2.2 Principles

The comprehensive information security management system at SURS is based on the recommendations of the information security standard of the International Organisation for Standardisation (ISO) 27001:2013 and is in line with the principles comprised in the European regulation governing European statistics, the requirements of the act governing national statistics, the

act governing personal data protection, the act governing confidential data and the regulations of the information security policy of the Ministry of Public Administration.

Each user is responsible for active cooperation in ensuring the information security, especially for dedicated reporting of the shortcomings noticed in regard to the activities on information security and breach of this policy and other rules on information security to their superiors or to the Information Security Officer.

Before commencing work at SURS, each user must be acquainted with SURS's information security policy and the duties and responsibilities related to information security. Each user at SURS must also be formally obliged to respect the information security policy.

The information security management system is based on continuous development, improvement, training of all the employees and increasing the general awareness of the importance of the information security at SURS. To this end, periodic training on information security is carried out for the employees and it is adapted in view of the risks that arise from the individual roles performed by SURS's employees.

The actions that are in contradiction with SURS's principles of information security represent a breach of the obligations at work. Breaches of this policy are viewed as breaches of the employment contract or another contract that governs the legal relationship on the basis of which a person gets access to SURS's information assets. The procedure is implemented in line with the regulations in force. When deliberating on the breaches and selecting the sanction the mode of breaching the policy, the seriousness of the breach, the number of breaches and other circumstances that are relevant for making the decision must be taken into account.

In case of serious breaches, SURS can use all the available legal means against those having committed a breach, including entering a criminal complaint in case of suspicion of committing a criminal offence or placing a claim.

The information security policy is subject to periodic reviews. It is supplemented and developed in line with other actual requirements of SURS. The sources of information for supplementing and upgrading the security policy can be:

- Feedback information;
- Security incidents;
- Results of independent reviews;
- Results of internal reviews;
- The efficiency of processes and taking into account the principles of information security during regular operation;
- Changes in the organisational environment, including changes in legal, business, technical and other conditions of operation;
- Tendencies of threats and vulnerability;
- Recommendations of the competent bodies.

Each time changes are made in the security policy and in individual subject-matter rules, SURS's users are to be informed via e-mail or with a release on the intranet or in some other appropriate way.

2.3. Documents on information security

The information security management system at SURS consists of security rules, instructions, operational procedures and guidelines. The information security policy is the basic document for the organisation of information security at SURS. Subordinate documents that regulate individual

procedures and measures related to the managing of information security are adopted on the basis of the security policy. These are:

- **Rules** on the use and management of information assets, how to protect them, security mechanisms and the level of security provided, adequate use of individual sources and the responsibility and roles of individual users in managing these sources;
- **Instructions** determining in detail the actions of users;
- **Operational procedures** comprising detailed rules on how to manage information assets;
- **Guidelines,** which are compilations of rules for a specific group of information assets or for a specific group of users.

2.4. Control environment and risk management

The security measures regarding SURS's information assets are based on the framework of risk management. Security of information assets is implemented in view of the exposure to risk. Information assets are exposed to various threats and such exposure poses also various risks to SURS.

The framework of risk management comprises the following elements:

1. Periodic assessment of risks of the security of information assets;
2. Assessment of the adequacy of the existing control environment in view of the risk assessment;
3. Treatment of risks – risks to which SURS's information assets are exposed are treated as follows:
   - by introducing or improving control activities with which the risk is diminished or the possibility of being able to identify the real threat in time is increased,
   - by consciously accepting the risks or
   - by avoiding the risks by terminating the activity linked to the risk.

SURS's risk management system provides continuous upgrading of internal control activities aimed at securing SURS's information assets.

2.5 Implementation of internal audits

To determine the success and efficiency of the implemented information security management system, an internal audit of information security procedures and measures is carried out at least once a year.

Internal audit is carried out by a group of auditors appointed by Director-General to conduct individual audits. Appointed to the group can be employees who have obtained a certificate of competence in auditing the information security management system. Internal auditors are led by the Information Security Officer as the lead auditor who obtained a certificate of competence in leading the audit of the information security management system.

The lead auditor prepares a draft audit program for next year by 31 December of the current year.

In implementing internal audit it must be provided that auditors do not assess the areas for which they are responsible.

After the audit the lead auditor prepares the audit report and informs the Director-General about audit results. Based on audit results, the Information Security Officer prepares draft measures. The system of audits ensures continuous improvement of information security.

3. INFORMATION ASSETS

3.1 Description of the information assets

SURS's information assets are:

- **Data and information:** all data and information that are stored in the databases, files on servers and workstations and all data that are kept in physical form, including the statistical data, results of statistical processing, personal data collections, documentary and archive material, system documentation, user manuals and instructions, all the documentation on the information security, associated rules, and other information and data that are directly or indirectly used in the operation of SURS;
- **Software:** system software, software intended for statistical processing, all the application solutions and development tools;
- **Information means:** information and communication infrastructure, data medium and other SURS's technical equipment;
- **Other information assets:** usernames, passwords, system settings, administrative sources and other information or confidential information to which SURS gains access during its operation.

3.2 Owner and administrator

Each information asset is formally assigned an owner and an administrator. Owners and administrators of the information assets must be documented and approved by SURS's Director-General.

4. HOW INFORMATION SECURITY IS ORGANISED

4.1 Roles and responsibilities

Director-General:

- Taking note of periodic reviews of the system and adoption of the changes and supplements of the documents from the field of information security policy;
- Providing financial, human and organisational resources to introduce, maintain and upgrade the information security management system;
- Taking note of results of information security audits;
- Appraisal of the efficiency of the information security policy and measures;
- Assigning the roles and responsibilities of users within the field of information security;
- Approval of the introduction of internal training programmes and increasing the awareness in the field of information security;
- Harmonisation of information security activities and measures in SURS's organisational structure;
- Providing the compliance of information security with legislation;
- Providing the compliance of information security with the regulations of the Ministry of Public Administration.

Information Security Officer:

- Checking the alignment of information security with the legislation, the information security of the European Statistical System, information security regulations of the Ministry of Public Administration and other information security standards;
- Periodic review and maintenance of policies, standards and instructions on information security and proposing changes and amendments;

- Coordination of the activities for maintaining and upgrading the information security management system ;
- Giving advice to the Director-General in the field of information security;
- Monitoring and introducing new developments in security mechanisms and procedures;
- Managing information security risks;
- Monitoring the implementation of information security policies and instructions;
- Managing security incidents;
- Active collaboration in the elimination of damage caused by security incidents, interruptions of operation and other events that could pose a threat to the security of information assets;
- Proposing and guiding activities for continuous operation;
- Reporting and proposing changes regarding continuous operation;
- Control of physical access to ICT equipment and remote access to SURS's information system;
- Reviewing audit trails;
- Cooperation in development projects to provide information security;
- Cooperation in managing changes related to information security management system or information security;
- Cooperation in the preparation and implementation of contracts with contractors as regards information security;
- Supervision of contractors as regards information security;
- Training of employees on the implementation of information security and continuous operation;
- Preparing the annual report on the situation regarding information security and security incidents;
- Regular reporting to the Director-General.

Security forum:

- Giving advice and providing support and information to the Information Security Officer for preparing policies, standards and instructions regarding information security and other information security activities and procedures.

Committee on Statistical Confidentiality:

- Preparing analyses and proposing decisions regarding access to confidential data under special conditions (scientific-research purpose);
- Preparing analyses and proposing decisions regarding transmission of personal data for surveying to external users;
- Dealing with issues and giving advice regarding statistical confidentiality of employees and other persons with access to confidential data;
- Dealing with issues and giving advice regarding the use of confidential data for statistical purposes;
- Dealing with issues and proposing solutions regarding requests by units for access to individual data that relate to them or were transmitted to SURS by them;
- Dealing with requests and proposing solutions regarding requests by institutions and other entities for access to individual data for using them to determine the rights and obligations of units to which the confidential data refer;
- Dealing with issues and giving advice regarding data publication and equal access of users;
- Dealing with issues and giving advice regarding other issues related to statistical confidentiality.

Head of the EDP Infrastructure and Technology Division:

- Providing adequate implementation of the necessary technological and organisational measures regarding the security of information assets;
- Active cooperation in the security forum.

Head of the service in charge of general matters:

- Providing adequate implementation of the necessary technical and organisational measures regarding the security of information assets.

Owners of the information assets:

- Classification of the information asset and demanding that it be placed in the adequate information environment;
- Forwarding requests for granting user rights to the administrator and supervision of the granted user rights;
- Identification and assessment of risks arising from unauthorised access to the information assets for which they are the owners;
- Prevention of disclosure of data prepared for publication before the publication date and provision of statistical protection for the disseminated data.

Administrator of the information assets:

- Provision and maintenance of adequate secure environment for information assets;
- Allocation of rights of access to information assets on the basis of the request of the owner of the information asset;
- Preventive actions in the field of information security;
- Active rectification of damages in case of incidents;
- Informing the Information Security Officer of identified security threats.

Heads of internal organisational units:

- Implementation of information security procedures and measures.

Employees, contractors and other persons with access to SURS's information assets:

- Respecting provisions and security standards determined by the information security policy;
- Data processing in an adequate security environment;
- Prevention of disclosure of data prepared for publication before the publication date and provision of statistical protection for the disseminated data;
- Reporting on identified security incidents;
- Use of information assets in line with the prescribed purpose of use;
- Attending information security training.

5. FINAL PROVISIONS

This information security policy shall come into force on the day following the day of its publishing on SURS's internal portal.

On the date of the entry into force of this security policy the Information Security Policy of the Statistical Office of the Republic of Slovenia (No. 007-47/2011/1 of 21 September 2011, amended by No. 007-47/2011/26 of 24 April 2015 and No 007-47/2017/1 of 29 November 2017) shall cease to apply.

Number: 007-47/2017/20
Date: 18 October 2018

Genovefa Ružić
Acting Director-General