REPUBLIKA HRVATSKA
DRŽAVNI ZAVOD ZA STATISTIKU

GENERAL INFORMATION SECURITY POLICY

Information security documentation

Version	Status	Date	Reviewed/Modified/Approved	Comment
3.0	Final version	26.07.2019.	Lidija Brković	Approved by Director General
3.0	Final version	22.07.2019.	Mira Talan	Legal harmonization
2.0	Archive version	21.03.2019.	Marko Krištof	Approved by Director General
2.0	Archive version	03.12.2018.	Mira Talan	Legal harmonization
1.0	Archive version	14.12.2017.	Gordana Hočuršćak	Version creation

1. Purpose

By introducing the General Information Security policy (hereinafter referred to as: Policy), the Croatian Bureau of Statistics (hereinafter referred to as: CBS) establishes guidelines for the Information Security Management System (hereinafter referred to as: ISMS) following good practices and regulatory requirements.

This document is intended for use by CBS employees and external partners within the ISMS scope, as well as others who prove to have a legitimate interest. Within the ISMS scope, each individual has defined place and responsibility, and is provided by availability of awareness, education and training. The ISMS owner ensures supervision and adequate disciplinary measures in case of the violation of rules.

By introducing ISMS, the CBS establishes a management system that will guarantee, through continuous improvements within the Plan-Do-Check-Act (PDCA) cycle, the security of information and technical resources that are used by employees or external partners within their duties or authorisation.

ISMS is defined through the guidelines of this Policy and detailed procedures described in subordinate documents. ISMS protects:

- Confidentiality (information is protected against unauthorised access)
- Integrity (to safeguard the accuracy and completeness of information)
- Availability (provides availability of information to authorised users when required)
- Authenticity (ensures that one's identity is the one that was claimed)
- Non-repudiation (guarantees one's inability to deny the performed activity or the receipt of information/data)
- Traceability (ensures that activity of the sole subject can be monitored)
- Reliability (consistent, expected behaviour and results).

2. Objectives of establishing ISMS

The main objective of establishing ISMS is to support the fulfilment of CBS's business goals, i.e. the information protection goals need to be harmonised with the CBS's business goals.

The aims to be achieved by applying ISMS are the following:

- Data protection and information system security, i.e. mitigation of operational risks
- Compliance with regulations in the Republic of Croatia

The Director General of CBS establishes the ISMS goals (hereinafter referred to as: the Director).

3. Roles and responsibilities

Responsibilities are specified in the following table:

No	Task	Responsibility
1.	Information security sponsorship	The Director
2.	ISMS policy	The Head of Information Security Management System Committee creates the policy (hereinafter referred to as: the Head of the Committee), the Director approves it
3.	Information Security Management System (ISMS)	The Head of the Committee
4.	Information security objectives proposals	The Head of the Committee
5.	Review of the contracts regarding information security	The Head of the Committee
6.	Management of ISMS documents	The Head of the Committee
7.	Assessment and treatment of information security risks	The Head of the Committee
8.	Correction and prevention measures	The Head of the Committee
9.	Control of ISMS records	The Head of the Committee
10.	Information security management system audit	Internal Audit Department
11.	Raising awareness and training of employees	The Head of the Committee

Coordination of activities in various organisational areas related to information security management is carried out on the Information Security Management System Committee sessions (hereinafter referred to as: the Committee).

Incident reporting is carried out with the intention to limit the damage caused by security incidents, tracking them and learning from them. All employees and all external partners must be informed about the procedures for reporting various incidents, violations, threats, and vulnerabilities. In the event of significant security incidents that may jeopardize the primary business objectives or the survival of the CBS, the Head of the Committee and the Director are immediately informed. Every individual possessing relevant knowledge and abilities who notices a security incident must try to limit the damage independently.

4. Responsibilities of the Director

The Director should review ISMS functionality at least once a year, but also in case of all significant business and organisational changes. The Head of the Committee organises the Director's review of ISMS. The Head of the Committee, Head of Administrative, Technical and Auxiliary Affairs Department and others also participate in the Director's review, according to the agenda. Input data include, among others, internal and external auditing reports, risk assessment results, risk solution proposals, a statement on risk appetite and a plan for the implementation of security measures.

5. Information Security Management System Committee

As a part of its regular tasks, this body must ensure a clear direction and dedication to the implementation of ISMS as well as to consider information security issues from the perspective of each organisational unit and to coordinate various initiatives. The Committee members are appointed from various organisational units upon the Director's decision. The Head of the Committee chairs the Committee.

The Committee has sessions at least twice a year, or more frequently if needed.

The Committee session minutes are sent to all parties involved and classified as **Confidential**.

6. Guidelines on information risk management

Risk assessment includes all resources identified within the scope of the system, threats that can jeopardize the system, the probability of occurrence of such an event as well as a severity of consequences. The risk assessment is conducted by business process owners and the Head of the Committee. The risk assessment is carried out at least once a year, or more frequently if changes in the environment have occurred that could have a significant effect on the results.

For each identified risk, a decision is made on the solution and reduction of the risk to a business acceptable level, based on the established criteria. Risks are managed according to business priorities and financial capabilities and attempts are made to reduce them as soon as possible to an acceptable level for CBS operations.

Business process owners are responsible in their organisational units for regular information risk management control and for harmonising required activities with prescribed procedures. Activity reviews are performed once a year during regular inspections, or more frequently if needed.

The Director specifies the level of risk appetite during ISMS reviews and approves all measures for which additional resources are needed.

7. Responsibility

All participants in the business process of the CBS, i.e. of the information system, are obliged to abide by the provisions of this Policy in the part which relates to them and in the manner prescribed by them.

8. Validity

This Policy comes into force and applies from the date of adoption.

DIRECTOR GENERAL

Lidija Brković

CLASS: 650-03/19-01/4

REF.No.: 555-13-02-01-19-2

Zagreb, 26 July 2019