ROMÂNIA

INSTITUTUL NAȚIONAL DE STATISTICĂ

ANEXA nr. 1b la ORDINUL nr. 1572/10.11.2022

INS Information Security Policy

B-dul Libertăţii 16, sector 5, Bucureşti. Tel: 021.318.18.24 021.318.18.42. Fax: 021.312.48.75 / 021.318.18.51 / 318.18.73. www.insse.ro

Contents

1 Introduction

The purpose of this Policy is to safeguard INS information assets, setting the framework for a secure environment.

This policy provides general principles, requirements and specific recommendations for the protection of integrity, availability and confidentiality of information assets, including hardware, software and information, networks and systems.

This policy establishes general roles and responsibilities for information security structure.

1.1 Scope

The Information Security Policy applies to all business functions and covers information systems, networks, physical environment, relevant people who support those business functions and data.

This policy applies to all INS employees and third party services providers.

The objective of this policy is to ensure security of INS assets, including networks, information systems, software, and data which must be protected from unauthorized use and disclosure.

This policy sets out the basic principles, objectives, organisation and responsibilities regarding the security of:

- Information on all media, including paper, and covers the physical security of such media as well as logical access to it
- Information Systems which handle such information when an Information System is provided, owned, managed or operated by an external party on the basis of a bilateral agreement or contract with INS, the terms of the agreement or contract shall comply with this policy.

Digital information is considered an important asset and must be appropriately evaluated and protected against all forms of unauthorized access, use, disclosure, modification, destruction, or denial.

Information security controls must be sufficient to ensure the confidentiality, integrity, availability, accountability and auditability of important information.

1.2 Management Commitment

The INS President formally endorses the following statement as Information Security Policy.

INS shall:

- regard its obligations on information security, i.e. confidentiality, integrity and level of availability of information as absolute and inseparable aspect of statistical confidentiality and quality of service
- take all necessary measures to ensure the statistical confidentiality of statistical data in compliance with *Regulation 223/2009 on European Statistics* as amended by Regulation 759/2015, with *Commission Regulation 557/2013 on access to confidential Data for Scientific Purposes*, *European Statistics Code of Practice* and any other legislation referring to statistical confidentiality in the domain of European Statistics.
- ensure that security issues are taken into account from the start of the development and implementation of its programmes, projects and activities
- develop, exercise and maintain its Business Continuity Management System
- ensure the protection of the privacy and the free movement of personal data in compliance with Regulation.
- foster proper initiatives to raise awareness of staff on the provision of this Information Security Policy, including roles, responsibilities, processes and control measures.
- regularly verify compliance with this policy through audit, review, testing, technical monitoring and enforcement or any other means deemed appropriate.

Policies and procedures for information security, including business continuity, shall be defined, documented, endorsed by the INS management, internally published and communicated to all staff and other relevant parties.

All Directors and Heads of Departments shall take actions for implementing this Information Security Policy provisions in processes within their business areas, by directing and supporting the staff to contribute to their effectiveness in terms of security.

This policy shall be reviewed yearly or when significant organisational changes related to information security occur.

All staff is formally required to comply with this policy and to carry out their responsibilities as defined.

INS Management understands the importance of protecting information assets and addresses this through Information Security organisational structures. Information Security Officer will coordinate information security activities.

ISO is supported in his work by various functions inside the entity: IS Monitoring Team, IT Technical Departments, Human Resources, Labour and Information Security.

INS Management is committed to continuously decrease risks by providing effective and cost-effective protection commensurate with the risks of its assets.

1.3 Overall Objectives

INS will protect all information assets under its control through the implementation of a set of well-balanced technical and non-technical measures.

The objectives of the INS Information Security Policy are:

- To define the scope of the information security management system
- To express the commitment of the management for information security
- To establish roles and responsibilities for information security
- To integrate all aspects of INS information security requirements and practices into a single coherent policy framework
- To provide a framework for future developments in information security in INS
- To assist in the continuous process of raising security awareness among INS personnel
- To ensure consistency with other processes established in INS that may involve a security element, including Business Continuity Management and Disaster Recovery.

2 Information and IT Security

2.1 Physical Security

INS shall steer the implementation of the necessary countermeasures to ensure the physical protection of data, processes and systems that meet the minimum physical security requirements in line with Physical Security Policy .

2.1.1 Physical Security Perimeter

Access in INS building is controlled and is restricted to permanent or temporary staff and authorised visitors.

2.1.2 Secure areas

The access in restricted zones is allowed only to authorized personnel based on individual access cards or physical keys and will be granted only on a business need.

A log is maintained for accesses in securized zones.

2.1.3 Security of equipment off-premises

Equipments, information or software must not be taken off-site without prior authorisation. Adequate protection must be applied to off-site equipment, taking into account the different risks of working outside INS's premise.

2.1.4 Secure disposal or re-use of equipment

All items of equipment containing storage media, including removable media, either must be checked to ensure that any sensitive data and licensed software either has been removed or securely overwritten prior to disposal or sending back for repair, or must be securely destroyed.

2.1.5 Clean desk policy

To minimise the possibility of data loss, theft or unauthorised disclosure, staff are required to adopt security-conscious practices in their workplace. This requires all sensitive data on physical media to be locked away when not in use (clear desk policy). Staff must assume that their workplace can be accessed by outsiders. They must therefore not leave their terminal logged on and unattended they must choose nontrivial passwords and keep them secure. In addition, PCs or workstations with access to sensitive data or being granted local administrator privileges are subject to enhanced access controls.

2.2 Asset Management

The data, processes and systems of INS are considered to be vital assets and shall be protected in a manner appropriate to their importance and value to the organisation. In order to establish and maintain the appropriate level of protection, these assets must be registered and classified.

2.2.1 Information classification

The following controls should be implemented:

All significant hardware and software assets associated with INS Information Systems shall be identified and recorded on asset register or inventory

All information systems and data must be assigned a confidentiality classification level and an integrity/availability classification level in line with the scheme defined in the Information Classification Policy

All physical media (e.g. printouts, CD-ROMs, backup tapes, etc.) shall be protectively marked and handled according to the classification level of the information contained as specified in the Information Classification Policy

Information assets shall be managed and controlled throughout their lifecycle (creation, storage, handling and disposal) in a manner appropriate to their security requirements.

2.2.2 Responsibility for assets

INS Information Security Policy is the framework for assuring confidentiality, integrity and availability of INS information assets.

For an efficient management of information assets, they must have a designated business owner and must be protected by in a manner commensurate with their business value and sensitivity.

2.3 Business Continuity

INS shall determine its information security requirements in case of operational disruption and document them in its Business Impact Analysis

A plan for BCP must be developed with the list of systems and facilities which should be restored in a timely manner set by the SLAs and BIA.

BCP tests should be executed at least annualy, are scheduled and coordinated by the ISO.

ISO coordinates the Business Continuity process.

2.4 Change management

2.4.1 Security requirements of information systems

System Owners must ensure that adequate security requirements are properly implemented accordingly to corporate policies and standards. Identification and management of information security requirements and associated processes must be integrated at early stages of information systems projects and justified, agreed and documented as part of the project documentation.

All proposals for new applications or major changes to existing applications must contain a section identifying the security risks and the counter-measures proposed.

All phases within an IT application/system lifecycle (from initiation to design, development, test, deployment, maintenance, operation and support) shall adopt appropriate counter-measures as determined by the process of Risk Assessment.

2.4.2 Software acquisition and development

The decision for acquisition or for in-house development of a software must be made based on a business case that supports the decision. The business requirements for new system/application must specify requirements for security controls.

A risk assessment will be performed for the future system/application to ensure that appropriate security controls are integrated.

All new information systems, or enhancements to existing systems, must be authorized by the Business Owner and the ISO.

2.4.3 Software testing and maintenance

For all business critical and sensitive systems, the development and testing facilities need to be separated from operational facilities. Furthermore, clear rules for the migration of software from development to operational status need to be defined and documented.

Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with the INS information security policy and information security requirements.

2.4.4 Authorization for Change

All changes to information systems, applications or networks should be approved by relevant positions prior to be made.

2.4.5 Configuration Management

All systems used by INS are configured only by the designated personnel.

Unauthorized changes to system configuration are prohibited.

2.5 Operational management security

INS shall ensure the correct and secure operation of information processing facilities.

2.5.1 Backup and Recovery

Back-up of INS data must be made to all relevant environments. All back-up media (tapes, disks etc.) must be clearly labelled and encrypted. Back-up data must be stored both in INS site and into an off-site location. Both INS site and off-site locations must implement security controls to protect the data from unauthorized access or environmental/natural threats. Off-site facility must be located away from the INS site to be unaffected if the INS site were to be seriously damaged (e.g. by fire, flood, earthquake or explosion).

Back-up media must be tested regularly to ensure that backed-up data can be recovered in case of an emergency.

2.5.2 Protection from malware

INS implemented measures to detect and protect information systems, applications and networks from viruses and other malicious software (e.g. Trojan horses, worms, viruses, etc.)

All INS equipments which allows are protected by antivirus software.

No software may be installed, stored or used on INS systems, unless it has been officially authorised

All data supports (USB stick, hard disks, CD/DVD-Rom, etc.) must be virus checked before being inserted into any INS system.

All incoming and outgoing mails must be scanned for inappropriate or malicious content.

An appropriate disclaimer must be assign to all e-mails that are sent outside INS network.

A system for managing spam messages must be in place.

All users are responsible for reporting any virus or malicious activity to the IT Helpdesk Team.

The IT Helpdesk Team is responsible for ensuring that all virus incidents reported by the users are recorded and investigated.

System administrators are responsible for:

- ensuring that antivirus software is installed on all user computers
- ensuring that virus definitions are current
- are responsible for the antivirus protection of the servers.

2.5.3 Segregation of duties and facilities

Duties and areas of responsibility must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of information systems.

Segregation of duties is used to divide the responsibility of the completion of a process into separate, accountable actions and to avoid conflicts of interests.

Development, test and operational facilities must be separated to reduce the risks of unauthorised access or changes to the operational system

Domains must be separated to reduce opportunities for unauthorised or unintentional modification or misuse of information systems. Separation of domains can be done based on trust levels (e.g. desktop domain, server domain, public access domain, etc.). The perimeter of each domain must be well defined, controlling traffic between domains using an active gateway (e.g. firewall, filtering router, etc,)

2.5.4 Logging and monitoring

To detect unauthorized information processing activities, INS must have and maintain a consistent approach to collection and analysis of logging and audit trail data like user activities related to sensitive information, exceptions and information systems security events use or faults in information processing facilities. Log information shall be kept for a minimum period of 3 months to assist in future investigations.

Loggings facilities and log information must be protected against alterations, unauthorized edition or deletion of log files. Measurement of storage capacity of the log file media must be done to prevent it is being exceeded, resulting in the failure of record events or over-writing of past recorded events.

The clocks of all relevant information processing systems for INS must be synchronized to a single reference time source to ensure the accuracy of audit logs.

All potential security breaches must be reported, recorded and investigated by the Investigation Team.

2.5.5 Third Party Service Delivery management

- Service Delivery – Services delivered by third parties involving accessing, processing, communicating or managing information or information processing facilities or adding products or services to information processing facilities must have appropriate integrated security controls. These security controls, the service definition and the delivery levels must be documented in service delivery agreements so as to ensure they are properly implemented, operated and maintained by the third party
- Monitoring and review of third-party services – The services, reports and records provided by the third party shall be managed by designated personnel, regularly monitored and reviewed, and audits shall be carried out regularly

2.6 Incident Management

Regardless of where they are detected, significant challenges to the security of INS information systems must be communicated in such a way as to enable the appropriate corrective measures to be taken in the most effective manner in agreement with the standard on *Information Security Incident Management* Policy

It requires:

- the establishment of appropriate process for reporting security incidents. This process must alert as soon as possible the correct stakeholders and ensuring efficient responses to those incidents
- stakeholders must assess each information security event and decide whether the event must be classified as an information security incident. Classification and prioritization of incidents can help to identify the impact and extent of an incident.
- the establishment of mechanisms that report on the occurrence and analysis of security incidents across the organisational structure, in order to ensure that appropriate corrective measures can be taken
- all staff within the organisational structure shall report any security weaknesses within systems or services to IT Help Desk.

Any breach of the Information Security Policies caused by an employee will be investigated and could be subject to disciplinary actions.

2.7 Access Control

2.7.1 Access to Information and Systems

A formal user registration and de-registration process must be to enable assignment of access rights, in accordance with the Access Control Policy

Access to systems and information is based on individual accounts and are limited to active accounts only.

The allocation and use of privileges must be restricted and controlled, reviewing its access rights at regular intervals following a formal process.

Access will be granted only on a business need.

The allocation and use of privileges like local admin rights for access to confidential information (C2 and C3) must be restricted, monitored and controlled.

The access rights of INS's employees and external party users to information and information processing facilities must be removed upon termination of their employment, contract or agreement, or adjusted upon change.

2.7.2 Remote Access

Remote access to INS network and resources must use VPN (Virtual Private Network) technology. Strong authentication, encryption and accountability mechanism must be in place.

Access will be granted only on a business need.

A set of controls must be implemented to assure this.

Access in certain applications is allowed only using virtual desktops.

2.7.3 Internet Access

Access to the internet through INS IT infrastructures are allowed to use it only for professional purposes using a PROXY Server.

Web filtering must be in place.

A set of controls must be implemented to assure this.

2.7.4 Mobile computing

Mobile computing devices (laptops, PDAs, mobile phones, smart phones and other mobile computing equipment) presents particular risks that must be mitigated by appropriate security measures

2.8 Security Awareness

All INS staff will be trained in security awareness as part of the new hire orientation process and regularly afterwards. Security trainings are organized by the HR and ISO.

3 Responsibilities

3.1 Overall Responsibilities

INS President is accountable for the security of the institution's information assets. INS President approves Information Security Policy and ensures the means for implementation. Enable the effective performance of the ISO's tasks and ensure that to the ISO is given sufficient autonomy, time, resources and support to carry out his responsibilities, including active support by top management.

INS top management is responsible for naming the owners of new assets and new owners for existing assets when required.

All INS staff is responsible for the practice of information security policies and procedures.

3.2 ISO

The ISO is responsible for:

- Coordinating the periodical review of IS standards implementation
- Communicate the action plan approved by the management
- Keeping evidence of company information assets and of their associated risks
- Performing the internal audit, reporting the findings and making recommendations
- Coordinate investigation team.

3.3 Investigation Team

The Investigation Team is responsible for:

- Analysing reported incidents
- Determining the incident nature and recommending corrective actions for preventing and solving information security incidents
- Following up the solving of incidents
- Analysing and reporting incidents to the management.

3.4 Asset (System) Owner

The System Owner is responsible for:

- Identifying and managing risks for their Information Assets
- Ensuring that only authorized personnel have access to Information Assets
- Ensuring that consistent local processes and procedures are developed, implemented, followed and regularly reviewed

- Monitoring and reporting on legislative, statutory and contractual compliance in relation to Information Assets
- Reporting incidents.

3.5 Asset Administrators

The Asset Administrators are responsible for:

- Providing technical input regarding the standard/framework
- Safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making back-ups so that critical information will not be lost.
- Reporting incidents.

3.6 Managers

Managers are responsible for:

- Coordinating processes/ procedures documentation
- Enforcing compliance to standard
- Reporting incidents
- Ensuring that their staff are aware of their security responsibilities.

3.7 Project Managers Responsibilities

Project Managers are responsible for introducing the security requirements in the functional specifications for all projects. They are also responsible to check if the solution implemented follows the required and agreed specifications.

3.8 Employees Responsibilities

All personnel have a duty to:

- safeguard hardware, software and information in their care
- prevent the introduction of malicious software on the organization's information systems
- report on any suspected or actual breaches in security
- compliance with INS security policies.

4 Terms and abbreviations

BCP - Business continuity planning

ISO - Information Security Officer

Information Asset (System) Administrator - the person responsible for overseeing and implementing technical and operational controls who has technical control over an information asset. One asset may have one or more administrators for different technical duties

Information Asset (System) Owner - individuals who have been allocated responsibilities and hold accountability for an information asset. He/she is responsible for ensuring that information assets are handled and managed appropriately. This means making sure that information assets are properly protected and that their value to the organisation is fully exploited.

PROXY Server - a dedicated computer or a software system running on a computer that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting a service

SLA - Service Level Agreement

VPN - Virtual Private Network

Document Control Sheet

Revision history

Version	Date	Revision
V1.1	12.06.2020	Periodical review
V1.2	23.06.2021	Periodical review
V1.3	08.11.2022	Periodical review

This document is owned and has been created by

Owner	Author	Date created

Distribution list

Recipient	Department	Date distributed

This document has been reviewed by

Version	Reviewer	Date reviewed

This document has been approved by

Version	Name	Signature	Date