Appendix 1 to Order no 15
of the President of the Medical Research Agency
dated 31 March 2022

Information Security Policy of the Medical Research Agency

Valid from:	
Version:	**1.0**

Declaration of the President of the Medical Research Agency

The implementation of the objective of the Medical Research Agency (hereinafter : the “MRA”) in the form of supporting innovative activities in health care, with particular emphasis on the development of non-commercial clinical trials and research experiments, is associated with the processing of information of significant importance for the health care system in Poland and the development of innovative technologies contributing to saving the life and health of patients.

Therefore, the information processed by the MRA is protected from breaching its confidentiality, availability, and integrity, in a manner consistent with the highest standards of information security management.

This Information Security Policy of the Medical Research Agency aims to define the basic assumptions of the Information Security Management System in force at the MRA, its main objectives and the security measures applied.

The Information Security Management System is implemented to, in particular, allow the MRA to achieve such an organisational and technical level that:

- warrants the best possible protection of information processed within the MRA activities;
- allows the development of the MRA activities and sets the highest standards in terms of supporting innovation in health care;
- ensures the integration of information security management processes with other MRA processes and tasks;
- increases the trust of stakeholders in the MRA and its activities in the context of the security of information processed by the Agency.

The Information Security Management System of the MRA has been developed in accordance with the provisions of generally applicable law and relevant regulations, standards and good practices, in particular in compliance with the ISO 27000 family of standards.

In view of the above, I represent that the MRA management:

- is fully involved in the creation and development of the Information Security Management System;
- provides all resources necessary for the proper functioning of the Information Security Management System;
- actively promotes information security issues among employees and provides the training necessary to comply with the requirements of the Information Security Management System;
- support all persons contributing to the effectiveness of the Information Security Management System.

Table of contents

Chapter 1

General provisions

Section 1

1. This Information Security Policy of the Medical Research Agency (hereinafter: the "Policy") defines the principles of the Information Security Management System in force at the MRA.
2. The Information Security Management System of the MRA constitutes an element of an overall risk-based management system relating to the establishment, implementation, operation, monitoring, maintenance and improvement of Information Security.
3. Each time the "Employees" are mentioned in the Policy and other documents of the Information Security Management System, such provisions apply accordingly also to other Users.

Section 2

The terms used in this Policy have the meaning as follows:

1) MRA – the Medical Research Agency;
2) System Administrator – the Employee or Organisational Unit entrusted with the supervision of the MRA ICT System;
3) Assets – everything that has value for the MRA. Assets are divided into information, data and so-called supporting assets (in particular equipment, buildings and premises, software, human resources);
4) Information Security – preservation of the Confidentiality, Integrity and Availability of information;
5) Availability – a property of information consisting in its availability and usefulness at the request of an authorised entity;
6) Security Incident – a single event or series of adverse, unexpected events that pose a significant threat of disrupting business activities, endangering security or violating applicable security rules;
7) Integrity – a property of information consisting in its accuracy and completeness;
8) Stakeholder – a person or organisation that can influence, is influenced by, or sees itself as influenced by a decision or activity of the MRA;
9) Organisational Unit – Department, Office or independent position that is separated in the organisational structure of the MRA;
10) Data Medium – a removable and portable device that allows its user to record, modify or read data, such as: a flash drive, a portable disk, an internal disk, a memory card, a magnetic tape, an optical carrier, etc.
11) Risk Assessment – an overall process of identifying, analysing and evaluating risk that is understood as the impact of uncertainty on particular aims and expressed as a combination of the consequences of an event and the probability of its occurrence;
12) ISMS Officer – the Information Security Management System Officer; a person appointed by the President of the MRA to supervise the implementation of the obligations arising from the ISMS adopted at the MRA;
13) Vulnerability – a weakness of an Asset or a group of Assets that can be exploited by a threat;
14) External Entity – a legal person, natural person or another entity providing products or services to the MRA on the basis of a contract or other legal relationship who is not an Employee, trainee, volunteer, apprentice, expert or contractor providing services on the basis of civil law contracts;
15) Confidentiality – a property of information consisting in the fact that such information is not made available or disclosed to unauthorised persons;
16) Employee – a person employed by the MRA on the basis of an employment relationship;
17) President of the MRA – the President of the MRA or a person authorised by him/her;
18) ICT System – a set of cooperating IT devices and software ensuring the processing and storage of, as well as sending and receiving data by telecommunications networks using the end device appropriate for a given type of telecommunications network. The ICT System includes, but is not

limited to, computer hardware, portable devices, system software, systems (subsystems), network, applications;

19) ISMS – the Information Security Management System;
20) Control Measures – elements of the management system, for example: processes, policies, devices, and practices that modify the risk (in particular, limiting the probability of the risk occurrence or reducing its potential impact);
21) Portable Device – an IT electronic device that allows its user to process, receive or send data without having to maintain a wired connection to the network, such as a laptop, smartphone, tablet or Data Medium;
22) User – an Employee, trainee, volunteer, apprentice, or a person performing tasks for the MRA on the basis of a civil law contract, entrusted with the processing of information in connection with the implementation of that contract, as well as a person entrusted with the processing of information on another basis;
23) Asset Owner – a Head of an Organisational Unit or another person mainly responsible for the management of a given Asset;
24) Risk Owner – a person responsible for the management of a given risk, with competence or obligation to take action in relation to the area managed by this person;
25) Threat – a potential cause of an unwanted security incident that may result in damage made to the ICT System or the MRA.

Section 3

1. The main objective of the ISMS is to protect the MRA information against threats posed by external or internal sources and to maintain the continuity of processes and tasks implemented by the MRA.
2. The objective, referred to in sec. 3(1) above, will be implemented, in particular, through:
    1) ensuring Information Security in accordance with generally applicable law and in a manner adequate to the results of the Information Security Risk Assessment, including by:
        a) physical, technical and organisational protection of the MRA Assets against unauthorised access,
        b) protection of the MRA ICT System against threats,
        c) securing the information processed by the MRA against its damage, unauthorised modification or destruction;
    2) implementation and maintenance of appropriate technical and organisational information security safeguards, including their regular testing, as well as the measurement and evaluation of their effectiveness;
    3) Information Security risk management;
    4) constant raising of Employees' awareness in the field of Information Security, including the development and conduct of training in the field of Information Security;
    5) determining roles and responsibilities related to ensuring Information Security, including the designation of Asset Owners and Risk Owners;
    6) ongoing supervision over the ISMS documentation;
    7) ensuring supervision and control in regard to compliance with the principles set out in the ISMS;
    8) Information Security management in relations with contractors and other External Entities, in particular through the use of confidentiality clauses in contracts;
    9) ensuring that information can be recovered in the event of its modification or destruction;
    10) ensuring the continuity of the MRA operations, including the continuity of information processing processes;
    11) an appropriate response to Security Incidents.

Chapter 2

The MRA as an entity and its background

Section 4

1. The MRA is a state legal entity referred to in art. 9(14) of the Polish Act of 27 August 2009 on public finance.
2. The MRA operates in particular on the basis of the Polish Act of 21 February 2019 on the Medical Research Agency (hereinafter: the "Act"), its implementing regulations and the Agency's Statutes.
3. The activities of the MRA include in particular:
   1) co-financing of scientific research and experimental development in the field of medical and health sciences and interdisciplinary projects selected through calls, with particular emphasis on clinical, observational, epidemiological and experimental trials;
   2) issuing opinions and appraisals in the fields of medicine and health sciences for public administration bodies or other entities under relevant contracts;
   3) initiating and developing international cooperation in the fields of medicine and health sciences as part of programmes referred to in art. 15(1)(1) of the Act;
   4) initiating and performing its own scientific research and experimental development activities.
4. The MRA's strategic lines of action are set out in its annual plan of activities.
5. The organisational structure of the MRA and the functioning of its particular Organisational Units are determined by its organisational regulations.

Section 5

The most important MRA Stakeholders are the following:

1) the Polish Minister competent for health matters;
2) entities participating in calls for proposals for the implementation and co-financing of a project, announced and conducted by the MRA;
3) entities that have concluded an agreement with the MRA for the implementation and co-financing of the project (beneficiaries);
4) the Information Processing Centre – a unit subordinate to the Polish Minister competent for higher education and science, responsible for technical and organisational support of the ICT System referred to in the Act;
5) other than the above-mentioned public administration bodies, in particular the President of the Polish Office for Personal Data Protection;
6) MRA Employees and other Users;
7) contractors and other External Entities;
8) press (media).

Section 6

1. Internally, the MRA's background consists, in particular, of the following elements:
   1) the organisational structure, taking into account the division of functions and defined roles and responsibilities;
   2) human resources;
   3) knowledge, competencies and good practices;
   4) IT infrastructure;
   5) premises and buildings;
   6) internal regulations and adopted standards and rules;
   7) organisational culture;
   8) internal and external communication.
2. Externally, the MRA's background consists, in particular, of the following elements:
   1) provisions of applicable law;
   2) political, economic, technological, social and health-related factors;
   3) relations and contacts with external Stakeholders (including public administration bodies, suppliers and other contractors);

4) the MRA's reputation.

3. The MRA analyses the internal and external background of its activities on an ongoing basis and uses the results of this analysis to plan and perform the tasks entrusted to it, including the development and updating of the ISMS.

Chapter 3
Scope of the ISMS

Section 7

1. The ISMS applies to all MRA Organisational Units and all processes and tasks carried out by the MRA.
2. This Policy applies to all Users.

Section 8

The rules set out in the ISMS apply to all:

1) information processed as part of the processes and tasks carried out by the MRA, regardless of its form and method of processing, owned by the MRA or entrusted to it under contracts or agreements;
2) Assets supporting information processing as part of the processes and tasks carried out by the MRA (in particular human resources, buildings and premises, equipment, Data Media, software, network infrastructure, organisational structure).

Section 9

Detailed information on the scope of the ISMS, the purposes of the use of information security safeguards and the methods of their implementation are specified in the Declaration on the application of safeguards under ISO/IEC 27001:2017.

Chapter 4
Roles and responsibilities under the ISMS

Section 10

1. Proper management of Information Security in the MRA is ensured by its organisational structure, which includes in particular:
   1) President of the MRA;
   2) ISMS Officer;
   3) Data Protection Officer;
   4) Heads of MRA Organisational Units and Heads of Departments;
   5) System Administrator;
   6) MRA Employees other than mentioned above and other Users.
2. Responsibilities and roles are assigned in a manner that prevents conflict between them and ensures the reliability and impartiality of the performance of Information Security-related tasks.

Section 11

1. The President of the MRA:
   1) provides the resources necessary for the proper functioning of the ISMS;
   2) makes strategic decisions in the Information Security management process;
   3) appoints the Data Protection Officer and the ISMS Officer;
   4) approves the ISMS documentation and its amendments;
   5) supervises and supports persons contributing to the achievement of the effectiveness of the ISMS;
   6) promotes continuous improvement of the ISMS.
2. The ISMS Officer:

1) is responsible for ensuring compliance of the ISMS with the relevant requirements, in particular with the requirements of the following standards: PN-EN ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 24762;
2) initiates and supervises implementation, corrective and preventive actions in the field of Information Security;
3) coordinates Information Security risk management processes;
4) supervises the development, review and updating of the ISMS documentation;
5) develops and conducts training in the field of the ISMS;
6) oversees the Security Incident management processes;
7) supervises or carries out ISMS audits and periodic reviews of the ISMS;
8) maintains a register of Assets;
9) issues opinions, guidelines and recommendations in the scope related to the operation of the ISMS;
10) is responsible for liaising with stakeholder groups or other specialised forums and professional associations in the field of Information Security;
11) takes action on other issues related to Information Security, to the extent not reserved by the functions of other persons.

3. The Data Protection Officer is responsible for monitoring and ensuring compliance of the MRA with personal data protection laws.
4. The System Administrator is responsible for managing the MRA ICT System.
5. The Heads of MRA Organisational Units and Heads of Departments:
   1) supervise the implementation of the obligations arising from the ISMS by the Employees subordinate to them;
   2) identify the Assets and evaluate their criticality level and classification;
   3) conduct Information Security Risk Assessments in their areas of responsibility;
   4) cooperate with the ISMS Officer, Data Protection Officer and System Administrator – within the scope of tasks implemented by them;
   5) manage the continuity of operations within their areas of responsibility.
6. The Employees:
   1) carry out the responsibilities arising from the ISMS within the scope of the tasks entrusted to them;
   2) inform immediately of all events affecting the Information Security risk, including in particular Security Incidents;
   3) cooperate with the ISMS Officer, Data Protection Officer and System Administrator – within the scope of tasks implemented by them;
   4) undergo mandatory training in the field of the ISMS.

Section 12

1. Detailed duties and powers of the Data Protection Officer are set out in the Personal Data Protection Policy.
2. Detailed duties and powers of the System Administrator are set out in the ICT Security Policy.

Section 13

The ICTS Officer may be a person who:

1) has appropriate professional qualifications and, in particular, professional expertise on the principles of Information Security or management of ICT Systems and the ability to fulfill the tasks specified in sec. 11(2) of this Policy;
2) has at least three years of experience in managing Information Security or ICT Systems.

Chapter 5
ISMS documentation

Section 14

1. The ISMS documentation at the MRA consists, in particular, of the following elements:
   1) Information Security Policy;
   2) Declaration on the application of safeguards;
   3) Personal Data Protection Policy;
   4) ICT Security Policy;
   5) Operation Continuity Policy;
   6) procedures, regulations, descriptions, instructions and methodologies specifying the detailed roles and responsibilities arising from the ISMS;
   7) forms and templates;
   8) documents constituting evidence of the expertise of persons involved in the management of the ISMS.
2. The allocation of the ISMS documentation and granting access to it are carried out on a “need to know” basis.

Section 15

1. The ISMS documentation is subject to protection, in particular against its loss of Availability, Confidentiality, Integrity and against its improper use.
2. The ISMS documentation is subject to periodic and ongoing review and updating, taking into account, in particular, changes in generally applicable laws, internal regulations, applicable standards and other security requirements or purposes.
3. Detailed rules for reviewing and updating the ISMS documentation are set out in the ISMS Performance Assessment and Improvement Procedure.

Section 16

1. All Employees, as well as other persons who gain access to information processed by the MRA, are obliged to read the Policy and other ISMS documentation with which they have been provided, and to comply with the rules set out in the Policy and such documentation.
2. The ISMS documentation may be made available to persons other than Employees only to the extent necessary for the proper performance of their tasks for the MRA.

Chapter 6

General rules of Information Security management

Section 17

All Employees are obliged to properly handle the information to which they have access, in particular to:
1) keep confidential information the disclosure of which would be contrary to the provisions of generally applicable law, internal regulations and agreements concluded by the MRA, or if such disclosure could expose the MRA to damage;
2) handle information, to which they have access in the course of their duties, in a manner appropriate to the category and level of protection of the given information;
3) comply with the principles set out in sec. 18.

Section 18

In order to ensure an adequate level of Information Security, the following rules must be applied:
1) liability for Assets – for each Asset, an Asset Owner has been identified, who is responsible in particular for the proper security of such an Asset;
2) only necessary access – the rights of access to information are limited only to such information as is necessary for the performance of the duties entrusted to a given person;
3) only necessary knowledge – MRA Employees have knowledge about information that is limited only to matters that are necessary to perform their duties;
4) security assurance – in order to protect information, at least one safeguard is used for each piece of information;

5) adequacy – the Control Measures that are applied by the MRA must be appropriate to the type of information and situation;
6) completeness – in order to secure information, a comprehensive approach must be applied, taking into account all elements of the information processing process.

Chapter 7
Asset management

Section 19

The MRA identifies information and other Assets related to information and to means of information processing, as well as develops, maintains and updates records of such Assets.

Section 20

1. All information created, transmitted and processed by the MRA is subject to protection.
2. The information referred to in sec. 20(1) above, owned by the MRA, is subject to classification by assigning to its particular groups a level of protection adequate to their importance and impact on the continuity of the MRA's operation.

Section 21

Detailed rules regarding the management of Assets, including identification, classification and recording of Assets, are set out in: the Procedure for identification and valuation of assets and information security risk management; the Procedure for classification of information and handling specific groups of information; and in the ICT Security Policy.

Chapter 8
Information Security risk management

Section 22

1. In order to ensure an adequate level of Information Security and to achieve the security objectives established by the MRA, a comprehensive information security risk management system has been implemented at the MRA.
2. The system referred to in sec. 22(1) above consists in particular of periodic and ongoing Information Security Risk Assessments, risk reporting, as well as the development of risk treatment plans.
3. The results of the risk analysis are taken into account in all processes under the ISMS.

Section 23

All Employees are obliged to:

1) take into account Information Security Risk while implementing their tasks, processes and projects, regardless of their type and stage of advancement;
2) inform, within the scope of their competencies, the ISMS Officer, Data Protection Officer and System Administrator about all events that may affect Information Security Risk.

Section 24

Detailed rules for Information Security Risk Management, including its assessment and the development of risk treatment plans, are set out in the Procedure for identification and valuation of assets and information security risk management.

Chapter 9
Human resources security

Section 25

1. MRA Human Resources Security Management involves taking appropriate action before, during and after termination or change of employment occurs.

2. When agreements with Employees or other entities are concluded, it must be ensured that these agreements include provisions specifying the obligations of the parties in the field of Information Security.

Section 26

1. Job applicants are subject to verification in accordance with applicable laws and internal regulations of the MRA, and taking into account the type of information related to their future duties that they will process, as well as the Security Risks of such information.
2. Before the Employee starts performing his/her official duties:
   1) the Employee who has not yet received the appropriate authorisation should not be present at the MRA premises without the supervision of an authorised person;
   2) the Employee must become familiar with the ISMS documentation and sign a declaration of acknowledgement of the documentation and obligation to keep confidentiality. That declaration will be then attached to the Employee's personal files;
   3) the Employee must undergo training in the scope of his/her duties resulting from the ISMS.

Section 27

1. Upon commencement of his/her work, the Employee will receive access rights necessary to perform the tasks entrusted to him/her.
2. In the event of a change in the terms and conditions of employment, access rights will be subject to appropriate modification.

Section 28

1. In the event of a change or termination of employment, the Employee's access rights will be changed or revoked at the latest at the time of, respectively, the change or termination of employment. Revocation or change of access rights applies to any type of access, including physical and logical (virtual) access.
2. In the event of termination of his/her employment, the Employee is obliged to return any MRA Assets that he/she holds.

Section 29

The principles on granting access rights, as well as on their modification and revocation, are set out in the ICT Security Policy and in the Physical and Environmental Security Procedure.

Chapter 10
Training

Section 30

1. The MRA has an Information Security training system in place.
2. The training covers, in particular, the following subjects:
   1) the ISMS, including the Employee's duties related to Information Security – conducted by the ISMS Officer;
   2) personal data protection – conducted by the Data Protection Officer;
   3) use of the MRA ICT System – conducted by the System Administrator.
3. The training should address, in particular, the following issues:
   1) Information Security threats;
   2) the consequences of a breach of the Information Security principles, including legal liability;
   3) the application of Information Security safeguards, including devices and software that minimise the risk of human error.
4. The training is conducted as:
   1) initial training – conducted at the commencement of employment;
   2) periodic training – conducted at specified intervals (by the organisational unit or the person responsible for a given training), aimed at reminding and updating the knowledge of the

participants on selected security issues;
3) improvement training – conducted in the event of significant changes in the ISMS or Information Security obligations.

5. Periodic training must be conducted at least once every 2 years.
6. Undergoing the initial training is necessary for a person to receive access to MRA Assets.

Chapter 11

Physical and environmental security

Section 31

1. The physical and environmental safety management system has been implemented to reduce the risks arising from physical and environmental threats and to prevent:
   1) unauthorised physical access, damage to and interference in information and means of processing information belonging to the MRA;
   2) loss, damage, theft or a breach of the Integrity of the MRA's Assets;
   3) disruption of the MRA's operation.
2. Physical and environmental security management is carried out at the MRA through, in particular:
   1) defining areas of physical security along with establishing and maintaining appropriate safeguards, adequate to the types of information and other Assets stored in a given area;
   2) control of the traffic of persons at the MRA buildings and premises;
   3) management of physical access to areas, premises and other information storage facilities;
   4) use of adequate environmental safeguards to protect information and other Assets stored in particular areas from destruction or damage caused by natural phenomena.
3. Detailed rules for physical and environmental security management are set out in the Physical and Environmental Security Procedure.

Chapter 12

ICT security

Section 32

In order to ensure an adequate level of security of the MRA ICT System, the following safeguards must be applied in particular:

1) access to the ICT System is limited only to the elements of this System necessary for the proper performance of tasks by the User;
2) access to the ICT System is granted, modified and revoked, as well as protected in accordance with an established set out rules;
3) Assets that are part of the ICT System are properly recorded, monitored and protected against their loss, damage, unauthorised modification or other violation;
4) malware protection is applied;
5) the procedures for implementing and modifying software have been defined;
6) the rules for handling Portable Devices, including Data Media, have been specified;
7) backups and archives are created and tested;
8) the rules for the supervision of services provided by External Entities have been set out;
9) the rules for managing changes made to the ICT System and its elements have been defined;
10) detailed rules for the management of passwords and other confidential authentication methods have been set out.

Section 33

Detailed rules for the security of the MRA ICT System and control of access to this system are set out in the ICT Security Policy.

Section 34

Detailed rights and obligations of the ICT System Users are set out in: the Regulations of the ICT System User and the Instructions for the use of Portable Devices, constituting annexes to the ICT Security Policy.

Chapter 13
Security Incident Management

Section 35

1. The purpose of comprehensive Security Incidents management lies, in particular, in ensuring a coherent and effective system for responding to such Incidents and in minimising the risk of their occurrence.
2. To this end, all Employees are obliged to inform the ISMS Officer of any events constituting or likely to constitute a Security Incident, or increasing the risk of a Security Incident occurrence.
3. Detailed rules for Security Incidents management at the MRA are set out in the Security Incident Management Procedure.

Section 36

The MRA Security Incident Management System is integrated with other systems for reporting breaches or suspected breaches, in particular with the internal breach reporting system and the information system on threats or breaches of personal data protection.

Chapter 14
Operation continuity management

Section 37

1. Operation continuity management in the area of Information Security is an element of the MRA's comprehensive operation continuity management system.
2. The main objective of the operation continuity management system in force at the MRA is to maintain its ability to properly and timely perform statutory tasks and to protect the organisation and its Stakeholders from the negative consequences of disrupting the operation continuity.

Section 38

1. Operation continuity management is based, in particular, on:
   1) impact analysis;
   2) risk assessment;
   3) defining specific requirements for a given area and processes, in particular resulting from generally applicable law, internal regulations, guidelines, standards or good practices;
   4) development and regular testing of operation continuity plans.
2. Detailed rules for operation continuity management are set out in the Operation Continuity Policy.

Chapter 15
Performance analysis and improvement of the ISMS

Section 39

The ISMS is subject to continuous improvement in order to ensure its adequacy and suitability for the implementation of the objectives referred to in sec. 3.

Section 40

1. The system of performance analysis and improvement of the ISMS consists, in particular, of:
   1) internal and external audits of the ISMS;
   2) internal audits;
   3) periodic reviews of the ISMS management;
   4) taking corrective action;
   5) review of the ISMS documentation.
2. Detailed rules for performance analysis and improvement of the ISMS are set out in the ISMS Performance Assessment and Improvement Procedure.

Chapter 16

Compliance

Section 41

1. The ISMS in force at the MRA has been developed in accordance with applicable regulations and the requirements of relevant standards and guidelines in the field of Information Security, including in particular the following:
   1) the Act and its implementing regulations;
   2) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation):
   3) the Polish Act of 10 May 2018 on the protection of personal data;
   4) the Polish Act of 6 September 2001 on access to public information;
   5) the Polish Act of 25 February 2016 on the re-use of public sector information;
   6) the Polish Act of 17 February 2005 on digitalisation of the activities of entities performing public tasks;
   7) the Polish Act of 26 June 1974 – Labour Code;
   8) the regulation of the Polish Council of Ministers of 12 April 2012 on the National Interoperability Framework, minimum requirements for public registers and exchange of information in the electronic form and minimum requirements for ICT systems;
   9) the regulation of the Polish Minister of Internal Affairs and Administration of 18 January 2007 on the Public Information Bulletin (pl. Biuletyn Informacji Publicznej);
   10) the following standards: PN-ISO/IEC 27001, PN-ISO/IEC 27002, PN-ISO/IEC 27005, PN-ISO/IEC 24762.

Section 42

1. The MRA identifies legal, regulatory and contractual requirements and other obligations related to Information Security on an ongoing basis.
2. For that ongoing identification and implementation of the requirements referred to in sec. 42(1) above, the Heads of Organisational Units are responsible within the scope of the areas managed by them. The Heads of Organisational Units may entrust the implementation of the obligation indicated in the previous sentence to persons subordinate to them.
3. The ISMS Officer, in cooperation with a person or an Organisational Unit performing the compliance function, will support the identification process referred to in sec. 42(2) above by constantly monitoring changes in the generally applicable law, internal regulations, standards and other sources of obligations in the field of Information Security.
4. The ISMS Officer maintains and updates a list of legal, regulatory and contractual requirements related to Information Security.
5. In the event of changes in Information Security obligations, the Organisational Units and the persons referred to in the above points of this section will inform each other of such changes. In such an event, the ISMS Officer will also inform about the introduced changes the Organisational Units whose activities may be affected by these changes.

Section 43

1. All Employees are responsible for compliance within the scope of their tasks and Assets entrusted to them.
2. The Heads of Organisational Units or persons designated by them supervise the Employees' compliance with the rules set out in the ISMS documentation.

Section 44

In relation to the performance of the tasks entrusted to them, the Employees are obliged to comply with intellectual property rights (including those related to the use of proprietary software) belonging to the

MRA and other entities, as well as to immediately inform the ISMS Officer and Legal Department about any violation of these rights.

Chapter 17
Relations with External Entities

Section 45

1. The MRA will be managing relations with External Entities in a manner that ensures the appropriate level of Security of Information and other Assets.
2. External Entities are required by the MRA to comply with the obligations and requirements related to ensuring Information Security, including compliance with this Policy and other documents relevant to the legal relationship existing between the MRA and a given External Entity.

Section 46

When determining the External Entity's responsibility for Information Security, the account has to be taken of the activities that take place at the MRA’s headquarters, as well as any situations in which information related to the MRA's activities is processed outside its headquarters (this includes, in particular, remote access to the MRA ICT System).

Section 47

Detailed rules for the management of relations with External Entities in the context of the ISMS are set out in the Guidelines for Information Security in Relations with External Entities.

Chapter 18
Final provisions

Section 48

Violation of this Policy and other obligations in the field of Information Security may constitute a basis of liability of the Employee or other User, in particular constituting criminal liability or labour and civil law liability, and it may also result in termination of the legal relationship existing between the Employee or other User and the MRA.

…….

First and last name

DECLARATION OF THE CONTRACTOR

I, the undersigned, herby represent that:

1. I have read the Information Security Management System documentation in force at the Medical Research Agency, i.e.: Information Security Policy.
2. I undertake to comply with all rules concerning the security of information and other assets of the Medical Research Agency specified in the Agreement, in the documents referred to in sec. 1 or otherwise specified by the Medical Research Agency, applicable to the legal relationship linking me with the Medical Research Agency, and in particular I agree to:
   a) comply with the [select appropriate] rules established at the Medical Research Agency:
      - permitted use of the Medical Research Agency's assets, including their protection;
      - personal data protection;
      - physical access;
      - access to and use of the Medical Research Agency's ICT system, including mobile devices;
      - other rules regarding ICT security not covered above;
   b) keep confidential any information received in connection with the conclusion or execution of the Contract;
   c) return to the Medical Research Agency any information provided, i.e. in particular: documents, materials and data, together with all copies and carriers on which the documents and data were recorded in electronic form;
   d) inform the Medical Research Agency of any violations or security risks;
   e) oblige its employees, collaborators and other persons through whom [entity data] will execute the Contract to comply with the security rules referred to above.

…… …….

City/town and date Legible signature (name and surname)