Information Security Policy

Jan Karski Institute for War Losses

Warsaw 31 July 2022

INTRODUCTION

The following document sets out the assumptions and unified strategy for information protection at the Jan Karski Institute of War Losses (ISL). It defines the objectives of information protection, the scope of this protection, assigns responsibilities and competences, and defines the structure tasked with implementing the information protection programme, as well as defining tasks for individual units of this structure.

This Policy is the main document of the established Information Security Management System.

THIS TRANSLATION IS PROVIDED ONLY FOR ILLUSTRATIVE PURPOSES.
IF THERE IS A DISCREPENCY BETWEEN THE ENGLISH AND POLISH LANGUAGE VERISONS, THE POLISH LANGUAGE VERSION HAS LEGAL EFFECT.

DEFINITIONS

Authenticity - ensuring that the identity of an entity or resource is as declared (authenticity applies to users, processes, systems and information).

Personal data - information about an identified or identifiable natural person ("data subject"), where an identifiable natural person is understood to mean a person who can be identified, directly or indirectly, in particular by reference to an identifier, e.g. a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person.

Declaration - a document that describes the objectives of the safeguards and the safeguards that apply to an organisational unit's ISMS.

Availability - the assurance of being reachable and usable on demand, at an assumed time, by an authorised party.

Integrity - ensuring that data has not been altered in an unauthorised manner.

Non-repudiation - ensuring that it is not possible for one of the actors involved in the data exchange to disavow its participation in all or part of the exchange.

Confidentiality - ensuring that information is not shared or disclosed to unauthorised persons or entities.

Processing of personal data - an operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, e.g. collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

GDPR - Regulation of the European Parliament and of the Council on the protection of individuals regarding the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Accountability - the property of a system to attribute a specific action in the system to an individual or process and to place it in time.

Risk - a future, possible event that, if it occurs, could adversely affect the achievement of the tasks or objectives of the ISL.

ISMS or System - the Information Security Management System.

Risk Management - coordinated activities to identify and analyse risks and, through the application of appropriate safeguards, minimise the risks posed by the risk to an acceptable level.

I. DECLARATION OF APPLICATION

The ISL Director, being at the same time the Administrator of the Personal Data processed at the ISL, fulfilling its obligations in the field of ensuring information security with regard to personal data and with the Regulation of the Council of Ministers of 12 April 2012 on the National Framework of Interoperability, minimum requirements for public registers and information exchange in an electronic form and minimum requirements for ICT systems (Journal of Laws 2017, item 2247, as amended), promotes and actively supports the principles of information processing adopted at the ISL. An expression of the commitment and support of the ISL Director to guaranteeing information security is the decision to implement, maintain and improve the ISMS developed based on the PN-ISO/IEC 27001:2017 standard. The adopted rules and principles of conduct apply to all ISL employees, service and supply contractors, as well as other entities cooperating with the ISL, which need to access data as part of the execution of concluded contracts and for the duration of their execution. The adopted rules apply regardless of the form of information processing. The responsibility for the preparation and maintenance of the ISMS, as well as the coordination of the actions taken and the continuous improvement of the ISMS lies with the team for the implementation and maintenance of the ISMS, appointed by the Director of the ISL.

II. INFORMATION SECURITY OBJECTIVES

The ISMS's purpose is to ensure the protection of personal data and other information processed at the ISL against all types of threats, both internal and external, to guarantee the availability, integrity, confidentiality, accountability and authenticity and non-repudiation of data. Ensuring that the processing of information is carried out in compliance with the applicable laws and contracts concluded in a manner that does not infringe on the rights and freedoms of persons. The security objectives established are in line with and support the strategic and operational objectives pursued by the ISL.

The main objectives of the ISMS include, in particular:

● establishing the most important principles in the field of information security,

● preparing ISL employees for appropriate information security behaviour,

● defining the responsibilities within the security system and the levels of information accessibility of the different groups of ISL employees,

● influencing the building of information security awareness among ISL employees.

The above objectives are achieved by:

- designating responsible persons to ensure the optimal division and coordination of information security tasks,

- obliging ISL employees who process data (regardless of the form in which it is processed) to provide the data with an optimal level of security,

- adopting the principles described in the document as binding for all ISL employees,

- the continuous improvement of the ISMS in accordance with the requirements of the Polish Standard PN-ISO/IEC 27001:2017.

III. CONTEXT OF THE ORGANISATION

The ISL, as a state budgetary unit, performs tasks resulting from the following legal regulations:

● Order No. 321 of the Prime Minister of 2 December 2021 on the establishment of the Jan Karski Institute of War Losses M.P. 2021 item 1126.

IV. EXTERNAL FACTORS

Within the framework of external considerations, the ISL takes particular account of:

● the applicable legal order and the need to ensure compliance with the applicable legislation,

● economic, technological, natural, cultural, social, and political conditions,

● the expectations of customers and counterparties that affect the way in which the ISL's strategic objectives are achieved,

● relationships and contacts with external public and private entities (including contracts with contractors and suppliers),

● the ISL's image.

V. INTERNAL FACTORS

Within the framework of internal determinants, particular consideration is given to:

● the ISL's organisational structure, the division of competences, established roles, and assigned responsibilities,

● the adopted objectives and directions for action and development,

● internal orders, regulations and adopted standards,

● the nature of the tasks and processes performed,

● the resources used for the effective implementation of the assigned tasks and processes (e.g. budget, knowledge, employees, ISL buildings and premises, and ICT systems),

● internal relations and communication (e.g. information flow in a traditional form and through the ICT system).

VI. STAKEHOLDERS

The adopted rules and principles for the processing of information apply to all ISL employees and service and supply contractors, as well as other entities cooperating with the ISL that, in the performance of contracts concluded with the ISL and for the duration of their performance, need to gain access to data.

The principles adopted apply regardless of the form of information processing. The stakeholders of the ISMS are, in particular:

- natural and legal persons who are ISL clients,
- ISL employees,
- government and self-government administration bodies, and
- entities performing tasks for and on behalf of the ISL, suppliers, and contractors.

VII. LEGAL BASIS

The basis for the development and implementation of this policy is:

● the GDPR

● the Act of 10 May 2018 on the protection of personal data (consolidated text of the Journal of Laws of 2018, item 1000 as amended),

● the Regulation of the Council of Ministers on the National Interoperability Framework minimum requirements for public registers and exchange of information in an electronic form (Journal of Laws 2017, item 2247), and

● National Standard PN-ISO/IEC-27001:2017.

VIII. SCOPE OF THE ISMS

The scope of the established ISMS includes:

- Information processed as part of all processes and tasks (processing activities) carried out in the ISL, both in a traditional form (including printed or written information on paper) and electronically and verbally transmitted, and

- Assets supporting the processing of information as part of the aforementioned processes and tasks performed, including staff (all ISL employees regardless of employment basis, trainees, interns, volunteers, and others), external entities performing activities for and on behalf of the ISL or having access to ISL information assets, ISL buildings and premises where information is processed, equipment, including computer hardware, mobile devices and other data carriers on which information subject to protection is stored, software, network infrastructure, IT systems, tool software constituting components of ICT systems used to process information. This Policy and the rules described in this Policy do not apply to information processed under the Act of 5 August 2010 on the protection of classified information (i.e. Journal of Laws of 2016, item 1167, 1948, of 2017, item 935.).

IX. CONTINUOUS IMPROVEMENT OF THE ISMS

Implemented and maintained at the ISL, the ISMS is subject to cyclical (at least once a year) reviews and is subject to surveillance audits and internal audits. It is based on a continuous risk management process implemented in accordance with the implemented Risk Management Manual.

X. CLASSIFICATION STRUCTURE OF THE ISMS DOCUMENTATION

Within the framework of the established ISMS, a three-level classification of security documentation defining the principles and modalities of information security management and the assets supporting the processing in question in the ISL is introduced:

1. within level I of the ISMS (documents of a public, publicly available nature)

are distinguished by:

a) the "Information Security Policy of the ISL" - the main document: the document overriding the other internal legal acts on information security in force at the ISL, collectively forming the security documentation, defining the general framework, directions, principles and requirements of information security at the ISL and the scope of security documentation at the other levels, introduced and updated in the form of an order of the ISL Director,

2. Within level II of the ISMS (documents made available to all employees of the ISL, trainees, interns, volunteers, in justified cases to selected persons and external entities performing activities for and on behalf of the ISL or having access to the information assets of the ISL), thematic policies are distinguished:

a) which detail the provisions of the ISMS Level I policy,

b) defining specific security requirements and rules in key areas of information security, and

c) defined and updated by the Director of the Jan Karski Institute for War Losses.

3. Within level III of the ISMS (documents dedicated to and made available to selected persons and entities on a "reasoned knowledge" basis) there are:

a) selected procedures and implementing instructions:

- specifying the principles and manner of implementation of the requirements in the areas regulated at ISMS Level II in a given organisational unit/by a given external entity performing activities on behalf of and for the benefit of the ISL, or

b) selected agreements with third parties.

4. The documents developed at the different levels of the ISMS complement each other, forming a comprehensive documentation of the ISMS at the ISL (security documentation):

1) the ISMS level I documentation is of a general nature and its provisions refer to the level II documents in which they are detailed,

2) individual level II documents refer to each other and to level III procedures and instructions, and

3) the procedures and instructions of ISMS level III detail selected issues identified within the level II documentation.

5. To ensure the relevance, adequacy and effectiveness of the internal security regulations in force, periodic reviews and updates of the above documentation are carried out. The principles and procedure for conducting the reviews of the ISMS documentation are regulated in the Information Security Monitoring and Supervision Policy.

XI. ROLES AND RESPONSIBILITIES IN THE FIELD OF INFORMATION SECURITY

ADO - Administrator of Personal Data – the ISL Director responsible for the implementation and ongoing supervision of the process of personal data processing, deciding on the purposes and means of personal data processing. The ADO ensures the security of information processing, with particular regard to personal data, through the application of technical and organisational measures adequate to the occurring risks and the category of protected data. In particular, the ADO must ensure the measures and resources enabling the implementation and maintenance of the ISMS, as well as safeguards of data against their access to unauthorised persons, taken by an unauthorised person, alteration, loss, damage and destruction.

DPI - Data Protection Inspector - a person appointed by the ISL Director to supervise the observance of personal data protection principles.

The DPI's duties include:

1. setting standards and scope of documentation of the ISMS,

2. participating in preparing and giving an opinion on the individual policies, procedures, and standards constituting the components of the applicable ISMS documentation or determining the managers of the relevant organisational units responsible for the aforementioned activities,

3. familiarising employees with the regulations and applicable rules for processing information, in particular, personal data,

4. keeping a register of processing activities and categories of personal data processing activities,

5. supervising the keeping of records of persons authorised to process personal data,

6. taking immediate action in case of receiving information about:

a. the malfunctioning of the system processing personal data, and

b. the occurrence of a situation indicating a possibility of a data security breach,

7. developing and implementing a training programme for employees involved in the processing of personal data on personal data protection regulations, and

8. participating in the process of assessing the effects of processing.

MANAGING STAFF - (Director and Vice-Director of the ISL, heads of organisational units) are responsible for ensuring and supervising the compliance of the tasks carried out in the organisational units subordinate to them with the applicable information processing rules. In particular, they are responsible for:

1. the timeliness of personnel and contact information of subordinate employees,

2. the validity and adequacy of authorisations to process personal data held by employees of organisational units subordinate to them,

3. the validity and adequacy of authorisations to work in IT systems held by employees of organisational units subordinate to them,

4. keeping the register of processing activities and categories of processing activities up to date in the scope assigned to the organisational unit,

5. managing subordinate employees' access to the premises,

6. informing the DPI well in advance of new planned processing activities,

7. determining the scope of data collection necessary for the assigned tasks,

8. determining the sensitivity and criticality of the collected data in terms of confidentiality, integrity, and availability,

9. the substantive correctness of the collected data created by the subordinate organisational unit,

10. determining the type of applications and computer equipment that are necessary for data collection,

11. preparing and submitting requests for the purchase of computer equipment, peripherals, and software, and

12. the ISA cooperating with the DSI if there is a security breach,

ISA - Information Systems Administrators - designated employees responsible for implementing and maintaining technical and organisational safeguards concerning information systems.

ISL employees are required to:

a. familiarise themselves with and apply the principles adopted in the Information Security Policy, and other policies, standards, and regulations that constitute ISMS documentation,

b. promptly inform the DPI of incidents or threats to the security of personal data,

c. protect information from unauthorised access, accidental or deliberate destruction, loss, or modification,

d. maintain the secrecy of information with which they have become acquainted in connection with their function or work,

e. protect equipment, computer printouts, and other media containing information,

f. connect the equipment to the LAN network on a regular basis to download, among other things, AV system updates,

g. maintain the secrecy of the passwords entrusted to them, information on the frequency of their change and technical details of the systems, even after the termination of their employment with the ISL, and

h. in accordance with the applicable security documentation for the dataset in question, notify the DPI and the immediate supervisor of:

● the disclosure or the possibility of disclosure of information to unauthorised persons,

● the unauthorised alteration of protected information or the possibility of unauthorised alteration,

● the destruction or the possibility of destruction of information, in accordance with the applicable security documentation for the system, notifying the ISA and immediate supervisor of:

● the blocking or possibility of blocking the operation of an information system processing information or preventing other access to it,

● the possibility of systems failures, and

● disruptions to the operation of information systems.

It is prohibited to:

● disclose information to unauthorised persons,

● disclose, transfer identifiers and passwords or use the authorisations, identifiers and passwords of other employees,

● take documents and assets outside ISL premises in contravention of internal regulations,

● copy databases or parts thereof outside the copies provided for in the security documentation,

● interfere with the operation of the information system or the ICT network,

● process information in a manner that may compromise data security,

● process content on workstations and publish content on the Internet that is contrary to the law or the norms of social coexistence,

● install software that is not related to the performance of official duties,

● interfere with the hardware configuration of equipment, or

● use business equipment contrary to the rules set out in the relevant ISMS documents.

XII. INFORMATION PROCESSING PRINCIPLES

With a view to the best possible security of information and the assets supporting its processing, the following information security principles are introduced for application:

1. The purpose limitation principle - personal data must be collected for specific, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. This purpose must be specified at the time of collection (Article 5(1)(b) GDPR).

2. The principle of lawfulness, fairness, and transparency - personal data must be processed lawfully, fairly, and in a transparent manner for the data subject. All information and communications relating to the processing must be easily accessible and understandable and in clear and plain language (Article 5(1)(a) and Recital 39 of the GDPR).

3. The data minimisation principle - only data which is adequate and necessary to achieve the specific, legitimate purposes identified at the time of collection may be collected. Personal data which is not relevant to the purpose of the processing, redundant, or no longer useful, e.g. due to their obsolescence, may not be collected (Article 5(1)(C) and Recital 39 GDPR).

4. The data accuracy principle - personal data must be correct and updated where necessary. Every reasonable step must be taken to ensure that personal data which is inaccurate in the light of the purposes of their processing is deleted or rectified without delay (Article 5(1)(d) GDPR).

5. The time limitation principle - personal data must be kept in a form which permits the identification of the data subject for no longer than is necessary for the purposes for which the data is processed. The storage of data collected, e.g. for the performance of a contract, should be terminated when the statute of limitations for claims or other legal rights and obligations expires (Article 5(1)(e) GDPR).

6. The integrity and confidentiality principle - personal data must be processed in a manner which ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, by means of appropriate technical or organisational measures (Article 5(1)(f) GDPR).

7. The principle of limited processing - the processor and any person acting under the authority of the controller or processor and having access to personal data must process the personal data only on instructions from the controller, by which is meant processing on the basis and within the scope of the granted authorisation or the concluded contract of entrustment of the processing of personal data (Article 29 GDPR).

8 The principle of accountability - all activities and decisions related to the ISMS must be documented. Data processing activities (decisions regarding the management of access to information or information processing resources) must be documented or result in the creation of records allowing the assessment of the compliance of actions taken with the adopted principles.

9. The principle of accountability - responsibility for processing activities, decisions on access to information, documentation, processes, and means of processing must be clearly assigned to employees or organisational units.

10. The need-to-know principle - the ability to access information only within the scope and scope of their official duties or contractual provisions.

11. The traceability principle - persons, processes, devices accessing information, or information processing resources must be unambiguously identifiable.

12. The authentication principle - mechanisms to control access by a person, process, or device to information or processing resources must use appropriate means of authentication and ensure the security of the authentication information.

13 The separation of duties – the separation of duties related to decision-making related to access to information and the resources used to process it from those related to its technical implementation.

14. The principle of data protection by design - the implementation of a new processing activity (using IT tools) must be preceded by a planning phase that includes an analysis of the risks involved and the incorporation of appropriate safeguards.

15. The principle of protection by default - by default, only those personal data which are necessary for each specific purpose of the processing may be processed. This obligation relates to the amount of personal data collected, the extent of processing, the duration of storage, and the availability of the data.

16. The principle of adequacy of safeguards - the safeguards in place must be adequate to the risks identified.

17. The principle of authorised access - the use of ISL information assets must be based only on a formal authorisation to use the selected assets.

18. Additional security rules may be set out in other documents forming part of the security documentation.

XIII. CONTROL OF ACCESS TO INFORMATION

1. Physical and logical access controls are in place to ensure restricted access to ISL information assets, including buildings and premises, equipment and IT systems only for authorised persons and entities.

2. Detailed rules for managing access to ISL information assets are regulated in the relevant policies relating to physical and environmental security and ICT security.

XIV. MANAGEMENT OF INFORMATION ASSETS

To ensure an adequate level of security for information assets, the assets in question are inventoried, classified, and managed in accordance with the applicable requirements for their protection.

XV. RISK MANAGEMENT

1. To effectively manage information security, it is required to undertake periodic risk management activities, in particular, in the area of estimating, i.e. identifying, analysing, and assessing information security risks, with a view to reducing and eliminating the risks in question.

2. Information security risk management activities include, in particular:

a) preparing and periodically updating risk management documents,

b) conducting periodic risk assessments,

c) handling risks,

d) taking corrective action.

3. Detailed rules on information security risk management are regulated in the Risk Management Manual.

XVI. INFORMATION AND COMMUNICATION SECURITY

1. As part of information and communication security management, actions are taken in the area of estimation and control of the risk of loss of confidentiality, integrity, and availability of information in connection with the use of Information Systems administered by the ISL and applications, computers and mobile devices, computer networks, and data transmission.

2. The activities in question must be undertaken, in particular, regarding the monitoring, improvement, and development of the ICT infrastructure.

3. Detailed principles and requirements of ICT security are regulated in the relevant ICT security policy.

XVII. PHYSICAL AND ENVIRONMENTAL SECURITY

1. Protection mechanisms in the area of physical and environmental security are in place to prevent unauthorised physical access, damage and disruption to information processing and information processing means and loss, destruction, damage, theft of ISL information assets.

2. Detailed rules on the management of physical and environmental security are regulated in the relevant physical and environmental security policy.

XVIII. ENSURING BUSINESS CONTINUITY

1. Planning, reviewing, ensuring, reviewing, and evaluating business continuity and dealing with emergency situations are undertaken in the ISL.

2. The details of business continuity management are governed by the relevant business continuity management policy.

XIX. RELATIONS WITH EXTERNAL STAKEHOLDERS' EXTERNAL STAKEHOLDERS

1. To ensure the protection of information assets made available to service providers, suppliers, and other external persons and entities performing activities in the name of and on behalf of the ISL or having access to ISL assets, rules of conduct are introduced for cooperation related to access to ISL information assets and the use of the services of the above persons and entities.

2. In the case of the performance of delegated tasks or the use of assets, including the processing of information entrusted by external entities by means of an appropriate contract or agreement, in addition to the requirements specified in the security documentation in force in the ISL, it is permissible to apply the requirements and security recommendations specified by the aforementioned external entities, as long as the indicated "external" requirements and recommendations do not lower the security level of the other information processed in the ISL.

XX. COMPLIANCE WITH LEGAL PROVISIONS

1. To avoid violations of applicable laws, statutory obligations, and provisions of concluded contracts and agreements, an ongoing analysis of the compliance of internal regulations, adopted security policies and their application with the aforementioned laws is carried out in the ISL, including identifying, documenting, and updating all relevant legal, regulatory, contractual requirements and the organisation's approach to complying with them.

2. This analysis also addresses compliance with legal, regulatory, and contractual requirements related to intellectual property rights and the use of proprietary software.

3. Heads of organisational units, within the scope of tasks performed in accordance with the applicable Organisational Regulations, carry out ongoing supervision in their units regarding compliance with legal and contractual provisions.

4. The ISL Administrator of Personal Data is responsible for ensuring compliance of personal data processing with personal data protection regulations.

5. The team for the implementation and maintenance of the ISMS, in cooperation with the managers of the individual organisational units of the ISL, periodically reviews internal regulations on information security in terms of their compliance with the law and contractual provisions, according to the principles and procedure defined in the Information Security Monitoring and Supervision Policy and dedicated procedures.

6. The Audit and Risk Management Coordinator must ensure periodic internal audits of information security, at least once a year.

XXI. BREACH OF INFORMATION SECURITY

1. The primary consequence of an information security breach is a reduction in the level of protection of the information processed and the assets supporting its processing in the ISL.

2. Anyone who has access to information and assets supporting its processing in the ISL (ISL employees, as well as interns, trainees, volunteers, contractors, and other persons and external entities performing activities for and on behalf of the ISL or having access to ISL information assets) has a duty to inform the entities responsible for ISL security of any suspicion/any identified security breach.

3. Failing to comply with the rules contained in the security documentation constitutes a breach of employee duties and may result in sanctions of a disciplinary nature.

4. Violating the provisions of the information security policy by an ISL contractor or its employees constitutes grounds for withdrawal from the contract and demand coverage of the resulting damage or payment of a contractual penalty, if such an obligation arises from the concluded contract.

5. The actions of ISL employees and contractors and other persons and entities referred to in clause 2, which are incompatible with the provisions of generally applicable law (those concerning the processing of personal data), are subject to separate penalties set out in:

1) the Labour Code,

2) the Civil Code,

3) the Penal Code, or

4) the Personal Data Protection Act.

6. To obtain the fullest possible information on a breach or suspected breach of information security at the ISL, persons or entities not related to the ISL may report cases or suspected breaches of security <kancelaria@instytutstratwojennych.pl>.

XXII. DEROGATIONS

Taking any action derogating from the provisions of this Policy requires the written consent of the ISL Director.