Information Security Policy

****

# Object of this document

Introduction of the Information Security Policy, hereinafter referred to as the Policy, is aimed at determining information security management processes. The Policy shall be the governing document in Information Security Management System. All principles specified herein contribute to improvements in the MDH business activity, providing the company's customers and contractors with the highest quality services delivered by MDH Sp. z o.o. hereinafter referred to as MDH.

# Scope of the document

All individuals involved in information processing taking place in MDH shall be obliged to follow the Policy principles along with the provisions specified in the related documents. Specific principles of the Policy can be also obligatory for other entities, which cooperate with MDH and process information.

# Declaration of the top management

Management Board in MDH hereby recognises the need to protect information and recommends effective security measures, mechanisms and processes. Information security management process is subject to constant changes, as a result of which the Board finds it indispensable to improve the system on a regular basis.

# Legal basis

* 1. Information Security Management System (ISMS) complies with applicable legal provisions observed by MDH, in particular:
1. Act of 10 May 2018 on Personal Data Protection.
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. Ordinance of the Council of Ministers of 12 April 2012 on the National Interoperability Framework, minimum requirements for public registers and information-sharing in electronic formats and minimum requirements for ICT systems.

# Definitions

* 1. Terms used in the Policy and the related documents shall be construed as follows:
1. **Personal Data Controller (PDC)** - MDH Sp. z o.o., determines the purposes and means of the personal data processing. PDC's tasks shall be performed by the top management i.e. the Management Board in MDH.
2. **IT System Controller (ITSC)** - the natural person or persons assigned by the Personal Data Controller, who shall be held responsible for observance and supervision over observance of the information security principles applicable within the IT system, covering their duties and authorisations. Different IT systems may be supervised by different ITSC.
3. **Information Security** - means confidentiality, integrity and accessibility of information.
4. **"Sensitive" data** - personal data subject to special protection, specified under Articles 9 and 10 of the GDPR. Discussed categories of personal data cover among others data concerning health, fingerprint data, data relating to criminal convictions and offences, etc.
5. **Personal data** - means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an on-line identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
6. **Accessibility** - guarantee, that all information remains accessible, whenever authorised entity needs to have it available.
7. **Incident** - (Information Security Incident) means a single, undesirable or unexpected event related with information security or a series of such events, as a result of which business activities are much likely to be disturbed or information security is likely to be put at risk.
8. **Data Protection Supervisor (DPS)** - the natural person assigned by the Personal Data Controller, who monitors, within his duties, observance of the personal data protection regulations.
9. **Integrity** - guarantees, that no information has been altered or deleted in an unauthorised manner.
10. **Personal data breach** – means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
11. **Authorised persons** - all natural persons, who in performing their professional duties have authorisation to process personal data or to whom such authorisation was granted, or who are authorised to process personal data under applicable provisions of law and personal data entrusting agreement. Authorised persons are entitled to process personal data.
12. **Entitled persons** - all natural persons, who in performing their professional duties are entitled to process personal data, or who are entitled to process personal data under applicable provisions of law and concluded agreements.
13. **Confidentiality** – guarantees, that no information is revealed to the third parties.
14. **Processing** - means any operation or set of operations which is performed on information, whether or not by automated means, such as 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.
15. **Data processing** - operations which are performed on personal data, such as collection, recording, storage, adaptation, alteration, making available, alignment and erasure, in particular if performed in IT system.
16. **GDPR** - 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.
17. **IT structure** - a set of technical devices and related security means i.e. hardware (PCs, printers, communications devices, along with related cabling and software) and software (operating systems, equipment software), as well as IT network and resources accessible thereby.
18. **IT system** – means software or a set of software which are used do process data in the common database, in particular with common users' authentication.
19. **Information Security Management System (ISMS)** – a set of all principles, procedures and processes aimed at guaranteeing information security.
20. **Act** - Act of 10 May 2018 on Personal Data Protection.
21. **Data erasure** - destruction of personal data or their modification to the extent, which make it impossible to identify the personal identity of the data subject.
22. **Data erasure** - destruction of personal data or their modification to the extent, which make it impossible to identify the personal identity of the data subject.
23. **User** – the natural person, who was granted authorisation in the IT system.
24. **Personal data set** - all structured set of personal data, which can be accessed according to some specified categories, whether the set is scattered or functionally organised.
25. **Event** – (Information Security Event) means identified occurrence of system, service or network condition, which suggests possible breach of the Information Security Policy or security failure, or event observed for the first time possibly related with information security.

# General information security principles

* 1. Information Security Management System and security measures are required by law, result from risk assessment concerning information security failure, as well as from monitoring carried out by the DPS, external/internal audits and Board's check-ups.
	2. Information security is achieved by means of organisational, technical, physical and business milieu security measures.
	3. Information subject to protection under ISMS documentation, shall mean personal data within the meaning of Article 4 of the GDPR.
	4. Provision of information security shall mean, that all information characteristics specified below are observed:
1. confidentiality - guarantee, that no information is revealed to unauthorised person,
2. integrity - guarantee, that no information has been altered or deleted in an unauthorised manner,
3. accessibility - guarantee, that all information remains accessible, whenever authorised entity needs to have it available.
	1. MDH observes the following security principles:
4. "Need-to-know principle" - entitled persons have access to information indispensable for their professional duties.
5. "Need-to-have principle"' - entitled persons have access only to these resources, which prove to be indispensable for their professional duties.
6. "Confidentiality principle" - entitled persons are obliged to keep in secret any information acquired in the course of performing their professional duties, as well as all information security measures applied in MDH.
	1. In all matters in dispute or specific requirements not determined in the ISMS documentation, departure from these principles need to be accepted by the Management Board or, where appropriate, by an immediate superior. All situations requiring departure from principles can form a basis for further development of documentation.

# Responsibilities in the information security procedure

## Personal Data Controller

* + 1. The Management Board (which performs PDC duties) - is responsible for providing all measures necessary to comply with legal requirements, approving ISMS documentation, assigning duties related with information security and supervising legality of personal data processing.
		2. The Board assigns Data Protection Supervisor and IT System Controllers.
		3. PDC's duties required by law, such as the impact assessment, performing information duty, execution of data subject's rights, shall be performed by the assigned persons and as specified in the the ISMS documentation.

## Data Protection Supervisor

* + 1. DPS shall have the following duties:
			- monitor the observance of the personal data protection regulations,
			- analyse and give opinions on risk assessment and data breach assessment,
			- monitor ISMS documentation,
			- supervise trainings provided for all persons involved in personal data processing, covering personal data protection legal requirements and principles,
			- provide his assistance to authorised persons and the Controller in terms of personal data processing and compliance with GDPR.
		2. To perform the aforementioned duties DPS shall be entitled to:
			- supervise persons involved in personal data processing in terms of appropriate use of personal data protection measures specified in ISMS and required by law,
			- give instructions to the persons involved in personal data security procedures, following advice from the Management Board, unless personal data security is at risk,
			- inform the Management Board on all personal data security breaches,
			- call all persons involved in data processing to provide explanations, when personal data security is breached, and to determine actual state of personal data protection.

## IT System Controller

* + 1. Depending of the scope of duties specified in the employment contract, ITSC shall be responsible for:
			- Doing or supervising repairs, maintenance works and disposal of computer equipment, where personal data is stored,
			- managing users' passwords and supervising observance of procedures determining acceptable frequency of password change in IT systems,
			- supervising actions performed in the system, concerning possible computer viruses, frequency of computer controls, as well as supervision over anti-virus software updates and configuration,
			- supervision over backing up and archiving backup databases, IT systems and other files,
			- supervision over check-ups, maintenance works and updates of the system designed for personal data processing,
			- supervision over proper functioning of the IT system,
			- granting authorisation, having collected BUM requests to authorise new employees,
		2. ITSC participates in the assessment of information security breach events related with IT architecture.
		3. Depending on the situation ITSC can be involved in the impact assessment in case of breach and analysis of the information safety impact, before new solutions are introduced.

## Business Units Managers

* + 1. The following duties refer to Business Units Managers (BUM), as well as other employees with the superior positions working with a group of other employees.
		2. BUM are responsible for:
			- taking part in the authorisation process and authorisation granting - including determining the scope of authorisation granted to dependent employees,
			- informing on any change of duties, which may influence the scope of authorisation or authorisation granted in the IT system,
			- supervising, whether dependent employees observe applicable principles,
			- taking part in the incident management process - including incident reporting and determining required actions to be taken,
			- analysing the impact of the changes to be introduced in MDH on the security of processed information,
			- analysing contracts to be concluded and outsourcing services in terms of personal data entrusting agreements.

## Entitled persons

* + 1. Entitles persons, including persons to whom authorisation was granted, shall be obliged to:
			- comply with the provisions of law and information security principles,
			- pay attention to any strangers, which happen to be present in the restricted areas,
			- inform on any events, which are likely to breach information security,
			- inform on drawbacks or improper functioning of security measures,
			- inform on any changes to the information processing processes or personal databases, including broadening or narrowing the scope of data processing, data erasure or the need to develop new processes and databases.

## Other employees

* + 1. Other employees, who are not involved in information processing, shall be obliged to:
			- inform on any events, which are likely to breach information security - e.g. documents left outside restricted areas, cabinets or in open space during the working hours, etc.
			- inform on improper functioning of security measures, in particular physical ones.

# Check-up and further development of the information security management system

* 1. ISMS is developed according to the Change Management Process and improvements introduced on the basis of the said process.
	2. Risk assessment concerning loss of information security is carried out from time to time, as specified in the risk and impact assessment procedure.
	3. Check-up is performed in-house through direct supervision of compliance with the approved principles, as specified in specific scope of duties, and as a part of incident management and change management procedures.
	4. Moreover, in-house and outsourced audits are carried out to verify information security. Results of the DPS's monitoring provide additional information on the security condition.
	5. Consecutive numbers of editions are introduced to develop ISMS documentation and guarantee its observance. Before a given principle is satisfied, it needs to be verified against the latest edition, as specified in the list of related documents, and clause 9.

# Related documents

Information security policy covers the following related documents:

* 1. Personal data security policy - 1st edition
	2. Instruction on the IT system management - 1st edition
	3. Incident management procedure - 1st edition
	4. Change management procedure - 1st edition
	5. Risk and impact assessment procedure - 1st edition

**Łódź, 25th May 2018**  **the Management Board:**

 Piotr Baczyński

 Anetta Włodarczyk

 Mariusz Gierałt