INFORMATION SECURITY POLICY

WITH REFERENCE TO PERSONAL DATA PROCESSING

in

Altertechnika Sp. z o.o./ Altertechnika LTD LP

Płock, 2018

CONTENTS

NS

§1.

The purpose of the Personal Data Security Policy, hereinafter referred to as the Security Policy, is to obtain an optimal and compliant with the requirements of applicable legal acts in the field of personal data protection, the method of processing in Altertechnika LTD. . L.P collection of information containing personal data.

§2.

Terms applied in the Security Policy mean:

1. Company -Altertechnika LTD. . . L. P with its registered office in Warsaw at the address 146 Radawicka Str.
2. Correspondence address: 09-400 Płock, 42 Bielska Str.,
3. personal data - any information regarding an identified or identifiable natural person,
4. personal data processing - collecting, recording, storing, elaborating , changing, giving access and deleting personal data , especially in the IT systems,
5. user - a person authorized to process personal data,
6. system administrator - a person authorized to manage the IT system,
7. IT sysystem - data processing system in Altertechnika, LTD, LP along with the human resources, technical and financial which provides and distributes information,
8. securing the ITsystem - should be understood as the implementation of the administrative, technical measures applied and protection against modification , destruction, unauthorized access to data and disclosure or acquisition of personal data as well as their loss.

INFORMATION SECURITY DEFINITION

§3.

1. Maintaning the security of the information processed by the Companyis understood as ensuring their confidentiality, integrality and access at the proper level . The measure of safety is the size of the risk relayed to the resource constituting the subject matter of this Policy.
2. The following is an understanding of the above terms in relation to information and application:
   1) Confidentiality of information - understood as the assurance that only authorised employees have access to information,
   2) Integrality of information - understood as ensuring the accuracy , completenessof information and the methods of its processing,
   3) Access to information - understood as assurance , that persons authorised to have the access to information and the relaled resources at that time, when necessary,

4) Risk management - understood as the process of identifying, controcontrolling, minimizing or eliminating risks related to security which may concern the IT systems.

3. Additionally, information security management is related with the assurance of:

1) Indisputability of reception - understood as the ability of the system toprove, that the recipient of the informationreceived it at the defined placeand time,
   2) Indisputability of sending - understood as the ability of the systemtoprove that the sender of the information actually sent it or enetered into the system at the defined place and time,
   3) Accountability of activities - understood as ensuring that all the activities relevant for information processing were registered in the system and it is possible to identify the user that performed the activities.

III. SCOPE

§4.

1. In the information system of a Unit, there is processed information applied to execute the tasks necessary to fulfill the rights or complete the obligation resulting from the provisions of law.
2. This information is processed, stored both in the form of manual as well as electronic .

§5.

Security Policy shall apply to:

1. personal data processed in the IT system,
2. all information concerning the data of employees of the Unit, including personal data of staff and the content of concluded employment contracts .
3. all data of job candidates collected at the recruitment stage,
4. information regarding the protection of personal data, including in particular the names of accounts and passwords in personal data processing systems,
5. register of persons authorised to process personal data,
6. other documents containing personal data.

§6.

1. The scopes defined by the documents of the Information Security Policy apply to the entire information system of the Unit in particular to:

1) all existing, implemented currently or in the future information systems as well as paper-version in which there is processed information which needs to be under protection,
2) all lokations of - buildings and rooms in which there is or there will be processed information which needs to be under protection,
3) all employees within the meaning of the provisions of the Labour Code, consultants, trainees andother persons having access to protected information.

2. All employees within the meaning of the Labour Code are obliged to apply the principles set out in the documents of the Security Policy, consultants, trainees andotherpersons having the access to informtion which is subject to protection.

§7.

Classified information is not included in the scope of this Policy.

IV. STRUCTURE OF INFORMATION SECURITY POLICY DOCUMENTS

§8.

1. The documents of the Information Security Policy establish management methods and requirements necessary to ensure the effective and consistent protection of the informationprocessed.
2. The set of documents of the Information Security Policy consist of the following:

1) This document on Information Security Policy,
2) Instruction for managing IT systems in the scope of security requirements for the processing of personal data, describing the manner of managing personal data processing systems in the Unit - Annex No. 1,
3) Instructions for proceedings in the event of a breach of personal data protection, describing the procedure of proceedings in situations of breach of the security of personal data resources, observed attempts to breach this security, as well as a justified suspicion of a forthcoming attempt of breach - Annex No. 2.

ACCESS TO INFORMATION

§9.

Before starting their job, all persons whose professional abilities are related to the access to personal data must undergo a special training on current legal regulations on personal data protection and the rules related to personal data protection in the Unit.

§10.

The scope of activity for a person authorised to process personal data should determine the scope of responsibility for the protection of personal data in the degree appropriate to the tasks of this person performed when processing this data.

§11.

Sharing the personal data with entities authorised to receive it, on the basisi of the provisions of law, can be provided if in a reliable manner they can justufy the need to possess this data, and the act of sharing it will not violate the rights and freedoms of persons, whose data they refer to.

§12.

The premises, in which the personal data is processed, should be locked in the duration of the absence of the persons employed to process the data, in a manner preventing third parties from accessing it.

§13.

Personal data shall be made available upon a written, reasoned request, which should include the information allowing for searching in the collection of personal data and indicating the scope and purpose.

MANAGING PERSONAL DATA

§14.

The administrator of personal data is Altertechnika LTD. L.P. represented by the President of the Management Board Altertechnika . LTD. Bernard Szymeon

§15.

1. The following are responsible for the security of the Unit's personal data, :

1) Personal data administrator - **Altertechnika LTD LP, represented by the President of the Management Board of Altertechnika LTD Bernard Szymeon**

2) Unit Information Security Administrator/Data Protection Officer - a person designated by the Administrator

2. Information Security Administrator/Data Protection Inspector of the Unit implementing the information security policy has the right to issue instructions regulating issues related to data protection in the structures of the Unit.

3. In the contracts concluded by the Unit, there should be provisions obliging external entities to protect the data provided by the Unit .

§16.

1. Acknowledging the documents specified in §8 p. 2 the employees of the Unit confirm with their signature on " Statement on compliance with the rules and regulations on personal data protection and on maintaining the confidentiality of personal data " (see Annex No.3) and provide the Information Security Administrator/Inspector of Personal Data Protection

§17.

Protection of personal data resoaurces of Unit as the whole against its unauthorised use or destruction is oneof the basic obligations of the Company's employees.

3. SCOPE OF RESPONSIBILITY

§18.

Each employee of the Unit is responsible for information security.

§19.

Information Security Administrator/Personal Data Protection Inspector in the Company:

1. is responsible for the implementation of the Act on the Protection of Personal Data in the scope regarding the Information Security Administrator/Inspector of Personal Data
2. supervises the physical protection of the premises, in which the data is processed as well as the control over the persons staying in the premises,
3. defines the strategy for securing the Unit's IT systems,
4. supervises the provision of emergency power supply to computers and other devices affecting the security of data processing,
5. supervises the repair, maintenance and liquidation of computer devices on which personal data are stored,
6. identifies and analyzes the threats and risk that may arise from processing the personal data in the Unit's IT systems,
7. determines the needs for the protection of IT systems , in which the personal data is processed,
8. supervises the security of data contained in portable computers, removable drives, palmtops, in which personal data is processed,
9. supervises the circulation and storage of documents and publications containing personal data,
10. monitors the operation of security guards implemented in order to protect personal data in IT systems,
11. supervises the functioning of authentication mechanisms of users in the IT system processing data and control access to data,
12. approves applications for granting the user an identifier and rights to access protected information in a specified/ given processing system,
13. notifies the system administrator about the necessity to create a user ID in the system and to change/grant the rightholder access to the system,
14. keeps records of databases in IT systems in which personal data is processed,
15. keeps records of persons employed in the processing of personal data in IT systems,
16. keeps record of placesof processing personal data in IT systems,
17. keeps a register of personal data collections of the Unit (processed using the traditional method or in IT systems).

§20.

The Personal Data Administrator is obliged to comply with all provisions of the Data Protection Act, in particular by:

1. determining the individual duties and responsibilities of persons employed in the processing of personal data resulting from the Personal Data Protection Act,
2. determining the buildings, rooms or parts of room, constituting the area, in which the personal data is processed using a stationary computer equipment,
3. familiarization of persons employed in the processing of personal data with the provisions applicable in this respect,
4. performing the recommendations of the Security Administrator of Unit's Information regarding the scope of personal data protection,
5. implementing and supervising compliance with the Information Security Policy,
6. implementing supervising compliance with instructions for managing IT system for processing personal data,
7. acting in accordance with the instructions in the event of a breach of personal data,
8. creating organisational and technical conditions enabling the fullfillment of requirements resulting from the application of Personal Data Protection Act,
9. responsibility for the substantive correctness of data collected in information systems,
10. determining, which persons and on what rights have the access to information,

The work of the Personal Data Administrator is supervised in terms of security by the Information Security Administrator.

§21.

The IT System Administrator is responsible for:

1. current monitoring and ensuring the continuity of the operation of the IT system and databases,
2. optimization of the performance of the IT system, databases,
3. network and server hardware installations and configurations,
4. installations and configurations of system, network, database software,
5. configuration of administration with system network and database software protecting data against unathorised access,
6. cooperation with service providers, network and server equipment and ensuring records regarding the protection of personal data,

7. managing backups of system, network software configuration,
8. managing emergency copies of data, including personal data and resources enabling their processing,
9. counteracting attempts to violate information security,
10. granting, at the request of the Data Administrator, , with the consent of the Security Administrator, information strictly defined rights to access information in a given system,
11. requesting information from the Security Administrator on security procedures and security standards,
12. managing of licences, and procedures concerning them,
13. running antiviral programmaes.

The work of Information System Admistrator is supervised in terms of security by Information Security Administrator.

4. PERSONAL DATA PROCESSING

§22.

1. Processing personal data takes place in determined/defined rooms whichwhich are locked by persons designated for this purpose.

The rooms in which personal data is processed, should belocked during the absence in them of the persons employed to process data, so that third parties are unable to enter.

§23.

1. Printouts, which contain personal data and are intended for the deletion should be destroyed to the extent which makes is impossible to read it.
2. Devices, disks or other data carriers, subjected to repair, prior to the repairshould be deprived of this data under the supervision of a person authorised by data administrator.

5. DEFINING THE TECHNICAL AND ORGANISATIONAL MEASURES NECESSARY TO ENSURE CONFIDENTIALITY OF PROCESSED DATA

§24.

There are the following categories of measures protecting personal data:

1. Physical security:
   - locked rooms,
   - locked armored cabinets,
2. Security of processing data processes in paper documentation:
   - the processing of personal data takes place in designated premises,
   - the processing of personal data is carried out by persons designated for this purpose.
3. Organizational security:
   - persons responsible for data security is the Information Security Administrator (ABl),Inpector for the Protection of Personal Data

     Information Security Administrator and all administrators called by him are controlling the work of the IT system with due diligence, in accordance with the current valid regulationsin this respect
     knowledge and with the applicable procedures,
4. Organization of work in the processing of personal data and principles of processing:
   - list of employees in the Unit authorized to process personal data, can be found at Information Security Administrator - annex no. 6
   - data can be processed only by employees, who have appropriate authorization granted by the Personal Data Administrator z .annex no. 5

- in the course of processing personal data, the employee is personally responsible for the security of the data entrusted to him,
  - before proceeding to the implementation of actions related to the processing of personal data, , the employee should check, whether the data held by him have been properly secured, and whether these safeguards are not violated,

- during the processing of personal data, the employee should take care of their proper protection against the possibility of view, or change by unauthorized persons for this purpose,
- after the processing of data has been completed, the employee should secure personal data against the possibility of access to them by unauthorized persons.

6. ARCHIVING OF INFORMATION CONTAINING PERSONAL DATA

§25.

Archiving of information containing personal data takes place in electronic and paper form. Data carriers are stored in separate rooms, which are protected against access to unauthorized persons (list of rooms annex no. 4)

INSTRUCTION FOR PROCEEDINGS IN THE EVENT OF PERSONAL DATA BREACH

in

Altertechnika LTD LP

§1

Instruction is intended for persons employed in the processing of personal data.

§2

A breach of the protection of personal data is acknowledged , when:

1. a breach of the security of the IT system or a breach of the security of a set of personal data collected and processed in another form has been found,
2. status of the device, content of the personal data set, disclosed working methods, manner of program organisation or quality of communication in the telecommunication network may indicate a breach of security of this data.

§3

Every employee of Unit, who finds or suspects a breach of personal data protection in an IT system (or processed in another way) is obliged to inform the administrator of this IT system or in
in the event of absence of the Unit's security information administrator.

§4

1. Personal data is disclosed, when it becomes known in whole or partially allowing to determine to unauthorized persons the identity of the person, whom data relates to.

2. In relation to data, which has been lost, left unattended outside the security area, there should be conducted explaining procedure, whether personal data should be considered as disclosed.

§5

1. The administrator of the personal data database, who has determined or obtained information indicating a breach of the protection of this database is obliged to the intermediate:

1) record all information and circumstances related to a given event, and in particular the exact time of obtaining the information about a personal data breach or after detecting this fact themselves,

2) if the system resources allow , generate and print all documents and reports, which can help in determining all the circumstances of the event, affix them with current dates and sign them,

3) identify the type of event that has occurred, including the determination of the scale of the destruction, methods of access to the data by the person unauthorised, etc.

4) take appropriate steps to stop or limit access to a non-qualified person, minimize the destruction and protect against termination of data breaches, including

a) physical disconnection of the device and segments in the network which can be used by an unauthorised person to access the database,

b) log out a user suspected of having a data breach,

c) change passwords to the administrator and user account by which illegal access has been obtained in order to avoid re-attempting of obtaining such access.

5) a detailed analysis of the state of the IT system in order to confirm or exclude the fact of a personal data breach,

6) restoration of normal operation of the system, whereby, if the database is damaged, restore it from the last emergency copy with all precautions aimed at avoiding re-access by persons unauthorised, in the same way.

2. Once the normal state of the personal data database has been restored, a detailed analysis should be carried out to determine the reasons for or suspected personal data breaches, and the necessary steps to eliminate similar infringements in the future.

3. If the cause of the event was of the IT user's mistake, there should be training to all persons/ recipients involved in data processing.

4. If the cause of the event was a virus infection, it is necessary to determine the origin of and to perform anti-virus protections and organizational protections that exclude the recurrence of a similar event in the future.

5. If the cause of the event was negligence on the part of the user of the system, the disciplinary consequences resulting from the Labor Code and the Personal Data Protection Act should be applied .

§6

1. The administrator of the personal data database, in which the personal data protection breach took place prepares a detailed report on the reasons, course and conclusions of the event and within 14 days from the date of its occurrence provides the administrator with security of information to the Unit. In addition, the Data Protection Administrator is obliged to raport within 72 hours to the President of the Personal Data Office and persons who are affected by the fact of a personal data breach

2. The information security administrator in the Unit performs analysis of reports and takes them into account in the preparation of the annual report for the Unit's data administrator.

LIST OF ROOMS, IN WHICH PERSONAL DATA IS PROCESSED, STORED, DESTROYED IN MKKM ltd:

a/ rooms located in office building in Płock at 42 Bielska Str.
rooms No. 4, 6, and 7

INSTRUCTION FOR MANAGING THE IT SYSTEM FOR THE PROCESSING OF PERSONAL DATA

in

Altertechnika Sp. z o.o./

Altertechnika LTD LP

SCOPE OF APPLICATION

The instruction defineS the rules for the management of the applied IT system for the processing of personal data, and in particular: the method of recording and of the deregistration of the user, of the passwords assignment and the rules for their use, procedures for the commencement of and termination of work, obligations of the user, methods and frequency of making copies, rules for checking the presence of viruses in computer and reviewing and system maintenance.

DATA PROCESSING AREA

1. The area of personal data processing with the use of stationary computer constitute the rooms presented in Annex 4.
2. All rooms that belong to the data processing area, are equipped with the lock. At the time of, when there are no authorized persons, the rooms are locked in manner preventing the unauthorised persons from entering. Non-authorized persons may stay in the data processing area only with the consent of the Data Administrator or in the presence of authorised persons.

III. REGISTERING AND DEREGISTERING A USER

1. IT system user can be (authorised person):

   a) a person employed in the processing of personal data in the Unit, who has the right to use the IT system and the devices entering its system,
   b) employee of another party or an enterpreneuer being a physical person and running a company enrolled to public enterprise evidence and who basing on proper contracts is performing services in IT business (maintenance, personal data processing order and others).

2. Obtaining the following permissions is available at two levels:

a) registration in a computer network (making an account),
b) granting specific rights to use the IT system.

3. Written request for registration of a user is submitted by the employee's direct supervisor. The applicacion is then submitted to the Information Security Administrator who can reject the permission, due to the threat of personal data security breach.

4. In case of termination of one's employment in the Unit, the following procedure of user's deregistration is applied :

1) on the employee's sign-off card, on which the person leaving collects signatures of the confirmation of settlement with the employer, there is an item stating the fact of removing or blocking the user profile,
2) Information Security Administrator as a person authorized to sign the sign-off card before signing the item stating the fact of removing the or blocking of the user profile issues an order to the system administrator to immediately perform this action,
3) after performing this action, the Information Security Administrator signs the sign-off card confirming the removal or blocking of the user profile,
4) performing this operation means preventing access to the system for employee, with whom the contract of employment in the Unit was terminated,

PASSWORD ASSIGNMENT METHOD AND RULES FOR USING THEM

1. Each time the user is authenticated in the system takes place after entering the login and password.
2. The use of password is mandatory for each user of, who has a login in the system.
3. In the Unit, the following rules for the use of password are obligatory:
    a) it is forbidden to disclose password to any third party,
    b) it is forbidden to write passwords or such dealing with them, which facilitates the access to a third party.

4. The proper enforcement of the obligations related to the use of the users' passwords is supervised by the Information Security Administrator/ Personal Data Inspector. This supervision in particular means observing (monitoring) the functioning of the authentication mechanism and restoring the correct state in case of irregularity.

COMMENCEMENT AND COMPLETION OF WORK

1. Before joining the IT system, the user is obliged to check the computer device and workstation with attention, or not circumstances indicating a personal data breach. In the event of a breach of personal data protection, the User shall notify the Information Security Administrator.
2. The user starts work in the IT system beginning with the following actions:

a) starting a computer ,

b) authentication ("logging" in the system) using login and password.

3. It is unacceptable to authenticate to the password and login of another user or work in an IT system on the account of another user.
4. The user's work in the system is commenced after "logging out" from thesystem. After the work is completed, the user secures his workplace, in particular, floppy disks, documents printouts, containing personal data, against access to persons unauthorized.
5. In the event of a long-term departure from the workplace, , the user is obliged to "log out " or activate the screen saver with option of re-doing "log in " to the system.
6. In case of irregularities in the authentication mechanism ("logging in " in the system), the user notifies the administratorabout them.

MAKING, STORING, VALIDATING AND DELETING BACKUP COPIES

1. Backup copies are made, stored and used taking into account the following rules:

a) copies are prepare on a daily basis on a separate server or external carrier,

b) copies are periodically, once a month, checked with regards to their suitability for restore data, and if their suitability ceases they are immediately deleted.

CHECKING THE PRESENCE OF COMPUTER VIRUSES

1. Checking the presence of viruses in the computer is done by installing a program that scans automatically, without the user's participation, all the files for the presence of viruses. The program is installed on all workstations.
2. After each repair and maintenance of your computer, it must be checked against the viruses and the antivirus program reinstalled.
3. Externeal electronic carriers of information are subject to checking with the anti-virus program before commencing using them. The data obtained by teletransmission should be placed - before opening - in the transient directory, which is subject to verification.

IV. METHOD AND DURATION OF STORAGE OF INFORMATION CARRIERS, INCLUDING COPIES OF IT SYSTEMS AND PRINTOUTS

1. Printouts and paper documents containing personal data are exclusively stored in separate lockers.
2. A person employed in the processing of personal data making a printout containing personal data is obliged to check the usefulness of the printout in the work performed, and in the case of its unsuitability - the printout is to be destroyed immediately.
3. Electronic information carriers with personal data are marked and stored in lockable cabinets or safes located in a special room, to which only authorized employees are available.
4. Physical liquidation of damaged or unnecessary electronic carriers of information with personal data is carried out in a way that makes personal data impossible to read.
5. It is permissible to order/entrust the destruction of any carriers of personal data to specialized external entities. The basis for the transfer of data for destruction to another entity should in each case be a contract concluded in writing.

V. RULES FOR VIEWING AND MAINTAINING THE SYSTEM

1. Review and maintenance of the data collections are made through:

a) checking the cohesion of database,

b) running queries to the database for data analysis,

c) viewing the printouts after designated processes,

d) checking the compatibility of data with documents,

e) analysis of the comments received by users.

2. Overview and maintenance is conduscted by an IT specialist in consultation with the Information Security Administrator / Personal Data Protection Inspector

3. In case of placing the order of performingacvtivities, beforementioned, to external entity, all works should be carried out under the supervision of the Information Security Administrator.

COMMUNICATION IN A COMPUTER NETWORK

1. With regard to the use of computer network in the Unit the following rules are obligatory:

a) employees are not authorized to install any private software. In the event that such software is installed without proper approval, the employee is responsible for bearing the organisational and legal consequences,

b) software on computers can be installed only by IT specialist,

c) employees do not have the right to transmit through the computer network to third parties any data constituting the identity of the Entity,

d) employees are forbidden to download any software via a computer network,

OBLIGATIONS AND RESPONSIBILITIES OF THE USER WITH REGARD TO THE INSTRUCTIONS

1. The user of the system is obliged to read the content of this instruction and confirm this with an appropriate statement.
2. Violation by an employee of this instruction may be treated as a violation of the obligations of employees and result in the employee's liability under the provisions of the Code of Work .
3. The content of this regulation is confidential, protected by the confidentiality of the employer on the basis of art. 100 § 2 point 4 of the Labour Code.