SECURITY POLICY

1) GENERAL PROVISIONS

The developed documentation defines the rules regarding the security of personal data processing in both traditional and paper collections as well as in electronic collections - processed in IT systems. The introduction of appropriate security measures, protection of personal data processing and reliability of operation are the basic requirements for today's IT systems. The following document presents in detail the mechanisms of data protection, as well as draws attention to the consequences that persons crossing certain limits may face. It also contains procedures for prevention and minimizing the effects of hazards.
The purpose of the Security Policy for the processing of personal data, hereinafter referred to as the Security Policy, is to define the directions of activities and support to ensure the security of processing personal data files managed by NAWITEL SP. Z O.O. SP.K. based in Bielany Wrocławskie, at ul. Atramentowa 10, 55-040 Kobierzyce, hereinafter referred to as NAWITEL SP. Z O.O. SP.K.
Security Policy is at NAWITEL SP. Z O.O. SP.K. the most important document defining the principles of data processing security, and all instructions and recommendations must be compatible with it. It applies to all employees, co-workers, people employed on a different basis than a contract of employment, contractors, contractors, consultants, apprentices, trainees and other employees who perform the tasks entrusted to them related to the processing of personal data.
The Personal Data Administrator manages the security of personal data through the use of data only for a specific purpose, which is necessary for the efficient performance of obligations under the law. In addition, it is necessary for the implementation of the contract or activities aimed at its conclusion, and the processing does not violate the rights and freedoms of the person to whom they relate, also at the time of consent.
The Security Policy is in accordance with applicable law, in particular with the Act of August 29, 1997, on the protection of personal data, as amended, and with executive acts issued on its basis.
Maintaining security processed by NAWITEL SP. Z O.O. SP.K. information is understood as ensuring its confidentiality, integrity and availability at an appropriate level, accountability, authenticity and non-repudiation. The level of procedures affecting data security is adjusted to the size of the risk. With regard to information and applications, these terms are defined as follows:
1) confidentiality - ensuring that information is not made available or disclosed to unauthorized persons, entities or processes,
2) integrity (data, system) - ensuring that the data has not been altered or destroyed
3) in an unauthorized manner, and the IT system functions intact, free from unauthorized intentional or accidental manipulation,
4) availability - ensuring that authorized persons have access to information and related information with it resources when it's needed,
5) accountability - ensuring that all activities relevant to information processing are registered in the system and it is possible to identify the user who performed the action,
6) authenticity - ensuring that the identity of the subject or resource is as declared (applies to users, processes, systems and information),
7) non-repudiation of receipt - assurance that at the time of data exchange the system is able to prove when and who participated in all or part of this exchange,
8) risk management - understood as coordinated activities of managing and managing an organization in the process of identifying, controlling and minimizing or eliminating security risks that may be related to information systems.

2) DEFINITIONS, STRUCTURE OF SAFETY POLICY SAFETY DOCUMENTS

The terms used in the Security Policy mean:
1) personal data - all information regarding an identified or identifiable natural person. A person identifiable is a person whose identity can be identified directly or indirectly, in particular by reference

to an identification number or one or more specific factors defining its physical, physiological, mental, economic, cultural or social characteristics.
2) personal data processing - it's any operations performed on personal data such as: collecting, saving, storing, developing, changing, sharing and deleting personal data, especially in information systems,
3) IT system - a set of cooperating devices, programs, information processing procedures and software tools used to process data,
4) securing data in the IT system - shall be understood as the implementation of administrative and technical measures ensuring data protection against modification, destruction, unauthorized access and disclosure, as well as unauthorized processing,
5) data set - it is every structured set of data of a personal nature, available according to specific criteria, regardless of whether the set is distributed (its parts are in different places) or functionally divided (processed using programs that perform various functions)
6) Personal Data Administrator (ADO) - an authority, organizational unit, entity deciding about the purposes and means of processing personal data. The data administrator is NAWITEL SP. Z O.O. SP.K., which bears full responsibility resulting from the provisions of the Act on the Protection of Personal Data in relation to the personal data files at its disposal,
7) ADO Representative - a person holding decision-making functions who, in the light of applicable regulations, has legal and actual influence on the processing of personal data and acts on behalf of ADO,
8) Personal Data Protection Coordinator (KODO) - it should be understood as a person designated by the Administrator of Personal Data to oversee compliance with security principles and security requirements resulting from generally applicable provisions on the protection of personal data,
9) IT System Administrator (ASI) - a person authorized to manage the IT system,
10) User - an employee or a person cooperating on the basis of a civil law contract authorized to process personal data.
The material scope of application of this Security Policy covers all personal data files processed in NAWITEL SP. Z O.O. SP.K., both in electronic and traditional (paper) form.
In the subjective scope, the Safety Policy applies to all employees
in NAWITEL SP. Z O.O. SP.K., and other persons having access to personal data, including trainees, people employed on the commission contract or contract for specific work, etc.
Classified information does not fall within the scope of this Policy.
The Security Policy introduces management methods and defines the necessary requirements to ensure effective and consistent protection of the information processed.

3) ACCESS TO INFORMATION

1. ADO shall apply access restrictions to personal data: legal (confidentiality obligations, authorization limits), physical (access zones, enclosing premises) and logical (restrictions on the rights to systems processing personal data and network resources in which personal data reside).
2. Every person who has access to personal data, before starting work, must become acquainted with the legal provisions regarding the protection of personal data and those in force at NAWITEL SP. Z O.O. SP.K. the principles of protection of personal data resulting from the Security Policy.
3. Only persons authorized by the Administrator of Personal Data may be allowed to process personal data. KODO keeps records of persons authorized to process personal data.
4. ADO authorizes the person to process personal data. Under this authorization, the person receives a unique ID allowing the processing of data in the IT system.
5. All persons admitted to the processing of data are required to read
and applying the procedures and measures introduced by the ADO that set out the principles of safe processing.
6. All persons admitted to data processing are obliged to sign a statement on familiarizing themselves with the provisions on the protection of personal data and on confidentiality.
7. Responsibility of the person authorized to process data in a given set should be appropriate for specific tasks performed while processing this data.

8. The presence of unauthorized persons in the area of personal data processing is allowed only in the presence of the User.
9. The sharing of personal data with entities authorized to receive it, under the law, should be carried out in accordance with separate procedural procedures.
10. Upon termination of the employment contract, contract of mandate / o work, the user's authorization to process personal data expires.

4) PERSONAL DATA MANAGEMENT

For the security of personal data processing in NAWITEL SP. Z O.O. SP.K. answer:
a) Representative of ADO (Personal Data Administrator) - President of the Board
b) Coordinator of Personal Data Protection (KODO),
c) IT System Administrator (ASI),
d) Members.

The ADO Representative appoints the Data Protection Coordinator (KODO) and a person authorized to replace the KODO. The substitute person performs tasks within the scope of KODO only when he / she is absent. In this case, at the time of the return, the KODO shall give him a report on the measures taken during the replacement.

Coordinator of Personal Data Protection at NAWITEL SP. Z O.O. SP.K. when implementing the Security Policy, it has the right to specify procedures and issue instructions regulating the protection of personal data in NAWITEL SP. Z O.O. SP.K.

Agreements concluded by NAWITEL SP. Z O.O. SP.K. on the basis of which personal data can be shared and processed, they must include an obligation on the external entity to comply with data security rules in accordance with the applicable rules and principles set out in this document. The person responsible for the contract reports the fact of entrusting the KODO data and completes the report. The rules of running projects and investments by ADO refer to the principles of personal data security and minimization of their processing.

Supervision of compliance with the rules on the protection of personal data arising from the Act the Personal Data Protection Coordinator exercises the protection of personal data, as well as other related legal acts and principles established in the Security Policy and Instruction for managing the IT system.

KODO is obliged to familiarize subordinate employees with the content of the Act of 29 August 1997 on the Protection of Personal Data (Journal of Laws of 2002 No. 101, item 926, as amended), Security Policy in the field of personal data processing, Instruction IT system management, used to process personal data and instructions for dealing with personal data breaches.

Getting acquainted with the documents specified above, employees at NAWITEL SP. Z O.O. SP.K. they confirm with the signature on the "Statement" and provide it to the Coordinator of Personal Data Protection.

Protection of personal data resources NAWITEL SP. Z O.O. SP.K. as a whole against their unauthorized use or destruction is one of the basic duties of employees. The obligation to keep the secret of personal data rests with all employees who have access to them, also after the termination of employment

.

5) SCOPE OF LIABILITY

Coordinator of Personal Data Protection:

1. Responsible for compliance with the Act on the protection of personal data in the scope regarding the Coordinator of Personal Data Protection;
2. Responds to familiarize Users with the content of the "Security Policy";
3. Implements and supervises compliance with the "Security Policy";
4. Monitors, and in the event of changes to the applicable law in the field of personal data protection, adapts the Security Policy to them;
5. With the help of ASI:
a) specifies a strategy for securing IT systems;
b) identifies and analyzes the risks and risks to which the processing of personal data in IT systems may be exposed;
6. Monitors the operation of security measures implemented to protect personal data in IT systems;
7. Supervises the security of data contained in portable computers, removable disks, portable memories and other media with the use of which personal data are processed;
8. Supervises the circulation and storage of documents and publications containing personal data;
9. Identifies individual responsibilities and responsibilities of persons employed in the processing of personal data. In the event of recruiting a new employee, changing the position, changing the scope of employee duties, creating a new set of personal data, changing the way of data processing is obliged to issue or withdraw the authorization to the User
10. Notifies ASI about the need to create a user ID in the system and to change or grant user access rights to the system and keep a record of changing passwords;
11. Supervises the functioning of user authentication mechanisms ·
in the IT system that processes data and data access control;
12. Receives from the Users a statement on getting acquainted with the Security Policy and Instructions;
13. Keeps a list of personal data files with an indication of the programs used to process the data;
14. Creates the organizational and technical conditions enabling compliance with the resulting requirements
from the validity of the Act on the Protection of Personal Data;
15. Records the consents given for the processing of personal data outside the designated area;
16. Records reports of entrusting personal data;
17. Keeps a register of service reports;
18. Keeps a register of backup copies;
19. Keeps a record of the destruction of backup copies;
20. Operates in accordance with the "Instruction in the case of a breach of personal data protection".

IT System Administrator
1. Responsible for the installation and configuration of system, network and database software;
2. Monitors and ensures the continuity of the IT system and databases;
3. Optimizes the performance of the database IT system;
4. Manages emergency data copies, including personal data and resources enabling their processing;
5. Supervises the provision of emergency power for computers and other devices affecting the security of data processing;
6. Supervises the repairs, maintenance and decommissioning of computer devices on which personal data are stored;
7. Together with KODO, identifies and analyzes the risks and risks to which the processing of personal data in IT systems may be exposed;
8. Identifies and informs the KODO about the needs in the scope of securing IT systems,
in which personal data are processed;
9. Carries out antiviral prophylaxis;
10. Prevents attempts to breach information security,
10.1.1. Grants strictly defined access rights to information in a given system,
10.1.2 Applications to the KODO regarding security procedures and security standards,

10.1.3 Manages licenses and procedures regarding them;
11. Carries out KODO commands regarding the application of the Security Policy.

User
1. Commits to apply the rules, procedures and guidelines set out by the ADO with a view to the proper and adequate processing of data;
2. It undertakes to keep confidential the content of personal data in legally protected secrets;
3. Responsible for substantive correctness of data collected in IT systems and in paper form;
4. Inform the KODO about all breaches of security rules and personal data protection
5. Asks the KODO to clarify doubts regarding legal provisions regarding the protection of personal data;
6. Carries out KODO commands regarding the application of the Security Policy;

6) REALIZATION OF THE RIGHTS OF THE PERSONS WHOSE DATA CONCERN

ADO shall take appropriate measures to provide, in a concise, transparent, easily understandable and easily accessible form, to the data subject any information referred to in Articles 13 and 14 of the RODO and communicate with it under Article . 15-22 and 34 RODO on processing.
Information shall be provided in writing or otherwise, including, where appropriate, electronically. If the data subject asks for it, the information can be given verbally.
ADO without undue delay, however, no longer than one month after receipt of the request, grants to the data subject information on the actions taken in connection with the request pursuant to Article. 15-22 RH0. If necessary, this period may be extended by another two months due to the complex nature of the request or the number of requests. The ADO informs the data subject about this extension, along with the reasons for the delay, within one month of receiving the request.
If the administrator does not act in relation to the request of the data subject, he shall immediately - not later than one month of receipt of the request - inform the data subject of the reasons for failure to take action and the possibility of lodging a complaint to the supervisory authority and use the means of protection before the court.
The data subject has the right to:
1. obtain from the administrator confirmation whether personal data concerning him is being processed, and if so, is entitled to access to them and information listed in Article 15.1
2. requiring immediate correction of incorrect data and supplementing of incomplete personal data
3. requesting the immediate deletion of personal data, and ADO is required to delete personal data without undue delay, if one of the circumstances set out in Article 17 of the RODO occurs
4. requests to limit processing in cases and on the terms set out in art. 18 of the RODO
5. receive, in a structured, commonly used machine-readable format, personal data about it that ADO has provided, and have the right to forward this personal data to another administrator without any interference from the ADO to whom this data was provided in cases and on the terms set out in Article .20 RHODE.
6. At any time, submit an objection - for reasons related to its special situation - to the processing of personal data based on art. 6 para.1 lit.e) or f) RODO. ADO may no longer process personal data unless it demonstrates the existence of valid legally valid grounds for processing that override the interests, rights and freedoms of the data subject, or the grounds for determining, investigating or defending claims.
7. ADO informs about rectification or deletion of personal data or limitation of processing, which he made in accordance with art. 16, art.17 paragraph 1 and art.18 of the RODO, each recipient who has been disclosed personal data, unless this proves impossible or will require a disproportionate effort. ADO informs the data subject of these recipients if the data subject requests it.

7) DATA SHARING

ADO provides personal data to persons or entities entitled to receive them under the law
ADO or a person authorized by him makes personal data from the files available in accordance with generally applicable regulations.
ADO may refuse to share personal data if it would cause a significant violation of the rights and freedoms of the data subjects or other persons.
In contracts concluded by ADO organizational units, in the event that it is necessary to entrust personal data to an external entity to perform the subject of the contract, provision is always made to entrust personal data. This fact requires the person responsible for the contract to complete the personal data and submit it to KODO.

8) CHARACTERISTIC OF THREATS INFRINGING THE PROTECTION OF PERSONAL DATA

Identifying threats that may affect the protection of personal data will help determine
and then introduce and monitor procedures to protect personal data.

1. Division of threats:
a) external threats (eg natural disasters, power outages), their occurrence may lead to the loss of data integrity, their destruction and damage to the technical infrastructure of the system, the continuity of the system is disrupted, confidentiality of data is not compromised,
b) internal random threats (eg unintended mistakes of operators, IT system administrator, hardware failures, software errors), data may be destroyed, system continuity may be disturbed, confidentiality of data may occur,
c) intentional, deliberate and intentional threats - the most serious threats to confidentiality of data (usually there is no damage to technical infrastructure and disruption of work continuity), these threats can be divided into:
• unauthorized access to the system from outside (burglary into the system),
• unauthorized access to the system from its interior,
• deterioration, quality of equipment and software,
• unauthorized transmission of data,
• Immediate threat to the material components of the system.
2. Cases classified as a breach or reasonable suspicion of a breach of securities collections in paper form and an IT system in which personal data are processed are mainly:
a) random situations or unforeseen impact of external factors on the system's resources, such as: gas explosion, fire, flooding, construction disaster, assault, terrorist activities, undesired intervention of the repair crew, etc.,
b) improper environmental parameters, such as excessive humidity or high temperature, strong electromagnetic field impact, shocks or vibrations from industrial devices,
c) hardware or software failure that clearly indicates intentional operation
towards a breach of data protection or even sabotage, as well as improper operation of the website, as well as the fact that the technicians are left unattended,
(d) the appearance of an appropriate alert message from that part of the system that provides resource protection or another message of similar importance,
e) the quality of data in the system or other deviation from the expected state indicating a system disruption or other extraordinary and undesirable modification in the system,
f) there has been a breach or attempt to breach the integrity of the system or database in this system,
g) an attempt or modification of the data or change in the data structure was found without proper authorization (authorization),
h) there has been unacceptable manipulation of personal data in the system,
i) disclosed to unauthorized persons, personal or secret data protection processing procedures or other guarded elements of the security system, e.g. user's login and password,

j) work in the system or its computer network shows non-accidental deviations from the assumed work rhythm indicating the breaking or abandonment of personal data protection - eg work at a computer or network of a person who is not formally authorized to operate it, signal of persistent unauthorized logging, e.t.c.,
k) the existence of unauthorized data access accounts or so-called "Backdoor", etc.,
l) personal data carriers have been replaced or destroyed without proper authorization or otherwise forbidden to delete personal data,
m) gross violation of the discipline of work in the area of compliance with information security procedures (no logout before leaving the job, leaving personal data in the printer, photocopying, not closing the room with a computer, work on personal data for private purposes, etc.).
3. The security breaches of personal data storage (open cabinets, desks, bookshelves, archival devices and others) on traditional carriers, ie on paper (printouts), film, film, photos, diskettes in the form of unsecured etc.

9) PROCESSING OF PERSONAL DATA

IT systems used to process personal data must meet the requirements of existing legal acts regulating the principles of collecting and processing personal data.
Individual archiving systems for individual processing systems are used to create backup copies of personal data in electronic form.
Safety copies and paper documents containing personal data are stored in conditions that prevent access to unauthorized persons.
Other information regarding the processing of personal data is contained in the IT System Management Instructions for processing personal data.

10) PERSONAL DATA SECURITY SYSTEM

By protecting data sets, it is meant to secure such information both during the introduction, processing in paper collections as well as in the information system and information carriers in order to protect it against illegal disclosure, theft and unauthorized modification or deletion. To this end, both the hardware and software mechanisms included in the IT systems should be used, as well as the procedures developed to increase data security.

Procedures that increase data security:
1. Personal data may be processed only by persons authorized to process personal data. Persons authorized to process data have the obligation to keep secret the data they process and the ways to secure them.
2. The person responsible for making modifications to the data set: structure, location, and creation of the collection is obliged to report this fact to the Data Protection Coordinator.
3. Personal data may be processed in rooms intended for that purpose.
4. Persons unauthorized to process personal data may stay in the processing of personal data only with the consent of the Data Protection Coordinator or in the presence of a person authorized to process personal data.
5. All rooms in which personal data are processed are locked, in the case of leaving the room by the last employee authorized to process personal data - this rule applies both at the end of work and during business hours.
6. Keys for business premises may only be taken by persons who are placed in the "list of keys to business premises".
7. Personal data in the traditional (paper) version is stored after finishing work
in lockable rooms and office furniture.
8. Keys from the cabinets should be protected against access of unauthorized persons to the

processing of personal data.
9. Data cabinets should be open only for the time needed to access data and then they should be closed.
10. Personal data in paper form may be on desks only for the time necessary to perform business activities, and then they must be stored in wardrobes.
11. Documents containing personal data, in exceptional cases with the consent of the KODO and after providing adequate protection, may be taken out of the place of processing. The employee who obtained the consent is responsible for the documentation. The consent is kept by KODO and provides instruction on information security.
12. Personal data in paper version, printouts and copies as well as in electronic version on CD, DVD, portable disks should be destroyed in shredders (or otherwise impossible to read) or forward to a hired company for destruction.
13. Cleaning of premises where personal data are processed is carried out after working hours by cleaning staff or persons designated for this purpose who have been familiarized with
with Security Policy procedures regarding them. Cleaning is done only
with the assumption that the "clean desk" rules will be kept by employees who process personal data. The "clean desk" principle is to protect personal data in paper form in time and after work in such a way as to make it impossible to read by unauthorized persons.
14. When processing personal data in ICT systems, the rules of a "clean desk" and a screen saver with individual password are used, setting up monitors in such a way that no information for unauthorized persons is visible.
15. When leaving the computer, one should log out of the IT System being used, and at the end of work, turn off the computer.
16. Only the persons authorized to do this have access to the rooms where the server and archive are located, especially those who have direct supervision of the server (ASI). The rooms should be secured by a door locked.
17. Near the entrance to the server room, the archive should have a fire extinguisher which is periodically filled.
18. The room in which the servers are located should be properly cooled, providing the right temperature and humidity for computer equipment.
19. It is forbidden to provide an individual ID and passwords to other people.
20. It is forbidden to delete data by throwing them into the waste bin.
21. It is forbidden to use private data carriers in systems processing personal data.
22. It is forbidden to use the public network (WWW) through unauthorized Internet browsers or unknown web sites, the content of which indicates a high risk of spyware, hacking, spammer and virus software.
23. In the event of request for data sharing, employees at NAWITEL SP. Z O.O. SP.K. they act in accordance with the provisions of the Act on the Protection of Personal Data, notifying the Data Protection Coordinator.
24. Data sharing is recorded in information systems, and in the case of traditional data sets, information on sharing is kept by the Data Protection Coordinator.
25. Detailed procedures for the management of the IT system are regulated by the "Instruction for managing the IT system used to process personal data".
26. Procedures applied to personal data processed in information systems
a) access control to personal data files;
b) individual user identifiers (employees processing personal data);
c) user authentication (confirming their identity);
27. In order to secure personal data against loss or damage, a number of physical, IT and organizational security measures are applied.
28. Users of systems processing personal data are subject to the following password policy:
— the minimum password length is 8 (eight) sign;
— the password contains uppercase and lowercase letters as well as numbers or special characters;
— storing passwords in a place inaccessible to other people;
29. A user who has lost his password is required to report this fact to the IT System Administrator immediately, who will set a new password;
30. Protection of data against loss of damage or unauthorized processing

In other cases:
a) In the case of repair, transfer, liquidation of the carrier (paper, hard disk, compact disc, portable memory, floppy disk, magnetic tape, etc.), which contains personal data to an unauthorized person to process data, a permanent erasure of information constituting personal data should be provided;
b) When using portable computers containing personal data, special care should be taken when using the computer outside of the data processing area;
In particular, it is necessary to use encryption mechanisms of files or databases embedded in the operating system. After the necessity of data processing on the portable computer ceases, it must be permanently removed from the data carrier;
c) The screens of computers on which personal data are processed are protected by password protectors. Monitors should be set up to restrict access to data to unauthorized persons for data processing;
31. Rules for sharing personal data between departments and employees:
a) Information containing publicly available data may be made available by the employee in the form of direct or telephone after verification of identity
in the "feedback telephone information" procedure;
b) On the other hand, access to personal data in a wider scope requires the consent of KODO.
32. Authorization to the collection of personal data as a substitute for a position: Authorizations for access and processing of personal data are related to the scope of performed duties and occupied position. When the employee is absent, a substitute person is appointed who is temporarily authorized to access and process data. Principle authorization as a substitute for a seat. The substitute person uses his own login and password to access the information system.

11) REVIEWS AND POLICY UPDATES

The Coordinator of Personal Data Protection analyzes the Security Policy at least once a year in terms of its suitability, adequacy and effectiveness.

The Security Policy is updated each time in the case of:
1. the liquidation, creation or change of the information content of the collection;
2. changing the location of the collection;
3. changes in the law on the protection of personal data, requiring the update of the Security Policy;
4. other significant changes concerning personal data in the functioning of NAWITEL SP. Z O.O. sp.k .;
The Security Policy update is made by the Coordinator of Personal Data Protection - with consent and in agreement with the Personal Data Administrator.

12) FINAL PROVISIONS

This Personal Data Protection Policy is announced in the company's enterprise and applies to both its employees, cooperating entities and proceedings towards contractors.
In matters not covered by the Security Policy, the provisions of the Act on the Protection of Personal Data, the Labor Code and other internal regulations shall apply.
Security Policy is stored by KODO.