HILLWOOD INFORMATION SECURITY POLICY

1. INTRODUCTORY PROVISIONS

1.1 The purpose of this Information Security Policy, hereinafter referred to as the "Policy", is to create management and regulation methods necessary to ensure an adequate level of security of Personal Data at every stage of its processing in information systems.

1.2 This Policy defines the method of managing the Information System with respect to Personal Data processing by the Data Controller, as well as by the persons authorized by it to process Personal Data.

1.3 The definitions used herein have the following meaning:

1.3.1 **"Data Controller"** means Hillwood,

1.3.2 **"IT Administrator"** means a person designated by Hillwood as the person responsible for ensuring the security of Personal Data processing in Information Systems,

1.3.3 **"Application"** means a part of the information system used by Hillwood to perform – in any manner – the function of collecting and processing Personal Data,

1.3.4 **"Personal Data"** means any information regarding an identified or identifiable living natural person,

1.3.5 **"Password"** means a sequence of letters, digits or other characters, known only to the User,

1.3.6 **"Identifier"** means a unique name of the User recognized by the Information System,

1.3.7 **"IT Infrastructure"** means, in particular, computer hardware, network devices, operating systems, system software,

1.3.8 "**Hillwood**" means Hillwood Development Company, LLC, registration number 800158445, a limited liability company registered in the state of Texas, United States of America, and its affiliated companies,

1.3.9 **"Data Protection Coordinator"** means the person responsible for the security of Personal Data processing by Hillwood in accordance with sec. 3 of the Hillwood Data Protection Policy,

1.3.10 **"Carriers"** mean all devices on which Personal Data is stored in electronic form, in particular: discs, CDs / DVDs, flash drives,

1.3.11 **"Personnel Member"** means a natural person cooperating with Hillwood under a contract of employment or any other contract, if it has not been concluded as part of the business activity carried out by that person,

1.3.12 **"Personal Data Processing"** means the collection, storage, analysis, use, disclosure, archiving or erasure of Personal Data and all other activities related to Personal Data (where the terms **Process**, **Processed** and **Processable** should be construed to imply the same),

1.3.13 **"Information System"** means a set of cooperating devices, software, information processing procedures and software tools used to process Personal Data,

1.3.14 **"User"** means a person who has access to the resources of the Information System under an appropriate authorization to process Personal Data,

1.3.15 **"Virus"** means unauthorized invasive software that causes disruption of the Information System.

2. SCOPE AND PURPOSE OF THE POLICY

2.1 The purpose of the Policy is to define the essential principles of proper management of the Information System used to process Personal Data at Hillwood and basic technical and organizational conditions that should be met by the devices and software components it comprises, adequately to the threats and categories of protected Personal Data.

2.2 The Policy applies to Personal Data processed in Information Systems and stored in an electronic form.

2.3 The Policy contains a specification of essential technical measures for the protection of Personal Data and elements of Information System management.

2.4 The Policy applies to Personal Data processed by the Company both when Hillwood is the controller of such Personal Data as well as in a situation where it processes such Personal Data under agreements for Personal Data subprocessing by third parties.

2.5 The obligation to comply with the provisions of this Policy applies to all Personnel Members of the Data Controller.

2.6 This Policy applies to all information Carriers on which protected Personal Data is or will be stored and all locations of the Data Controller – i.e. buildings and premises in which Personal Data subject to protection is or will be processed (in the future).

3. SECURING PERSONAL DATA IN INFORMATION SYSTEMS

3.1 Ensuring the security of Personal Data should be one of the most important factors in the selection of software comprising the Information System, which is to be used to process Personal Data.

3.2 In order to maintain an adequate level of security of processing Personal Data, access to the Information System processing Personal Data should be possible only after providing

the Identifier separate for each Information System User and the confidential Password or other element of authentication.

3.3 An adequate level of security of the Information System used to process Personal Data is ensured by observing the following rules:

3.3.1 preventing third parties from obtaining unauthorized access to the Information System,

3.3.2 installing or updating software only by persons or entities authorized to do so,

3.3.3 refraining by Information System Users from attempting to test, modify or breach security of that system and from any like activities.

4. GRANTING, CHANGING OR REMOVING AUTHORISATIONS IN INFORMATION SYSTEMS

4.1 General rules:

4.1.1 an authentication system is used in the Information System for processing Personal Data,

4.1.2 each person authorized to process Personal Data has a relevant Information System User account with relevant authorizations,

4.1.3 when creating a new Information System User account, a unique account Identifier is assigned which cannot be repeated for any other Information System User in the entire life cycle of the information system in which the Identifier was assigned,

4.1.4 the Identifier enables performing activities in accordance with the scope of entrusted duties, which determine the level of authorizations of a given User,

4.1.5 the procedure of granting authorizations to process Personal Data in the systems applies accordingly in the event of a change of authorizations in Information Systems or in the event of revoking authorizations in such systems,

4.1.6 changes concerning the Information System User, such as termination of a contract of employment or a civil law contract under which the cooperation with the Data Controller was established result in immediate de-registration of the Information System User and invalidation of the Password and recording this fact in the register of persons authorized to process Personal Data,

4.1.7 access rights granted to Information System Users who are not regular Personnel Members of the Data Controller should be temporary and may only be granted for a period corresponding to the task being performed and should be formally approved,

4.1.8 after exceeding the maximum number of authentication attempts in the Information System, the account should be locked and will require additional action (i.e. assistance from IT. with proper authentication) to be unlocked.

4.2 Management of Information System User accounts:

4.2.1 an Information System User account should contain the appropriate Identifier and be secured by a temporary Password, the change of which is required after the first login of the Information System User,

4.2.2 the same Identifier must not be used by more than one Information System User, with the exception of service accounts to which more than one person may have access. The password is stored in an encrypted database together with a list of persons authorized to download that password,

4.2.3 the Password authorizing the Information System User to use the Application is personally entered by the Information System User,

4.2.4 access rights granted in the Information System are determined by the actual official duties of a Personnel Member,

4.2.5 change of passwords of the Information System User is forced every 90 days (for 12-character minimum passwords), up to 1 year (for 16+ character passwords)

4.2.6 Passwords should consist of at least 12 characters, including an uppercase and a lowercase letter, a digit and a special character, and no commonly-used or 'dictionary' words

4.2.7 the Password may not be disclosed even after it loses its validity,

4.2.8 it is forbidden to write Passwords down, in particular to store them in places where they can be read by third parties.

4.2.9 In relation to systems that do not require changing the password, the user is obliged to change it at least every 90 days, with the exception of service accounts.

4.3 Rules for creating and using passwords in Information Systems.

4.3.1 system Users should select Passwords which must:

a) have a length of at least 12 characters,

b) contain lowercase and uppercase letters, a digit and a special character.

c) Passwords must not contain names, surnames, pseudonyms, initials and other combinations of characters or commonly-used or 'dictionary' words that could result in the passwords being easily decrypted by unauthorised persons,

d) the initial password which is assigned by the System Administrator allows the Information System User to register in that system only once and should be immediately changed by the User,

e) any hardware or software devices that initially had a default password should have them changed in accordance with the accepted requirements for creating passwords,

f) a repeated or recurring use of Passwords that have already been used should be avoided,

g) Passwords which have been suspected of being disclosed are subject to change without delay.

5. OBLIGATIONS OF INFORMATION SYSTEM USERS

5.1 Users:

5.1.1 comply with the rules for the protection of Personal Data set out in the Policy

5.1.2 are obliged to read the Policy – before being allowed to process Personal Data – and make a relevant statement confirming the knowledge of its content,

5.1.3 process Personal Data in accordance with the provisions of law and regulations in force at Hillwood,

5.1.4 inform the Data Protection Coordinator of any observed irregularities resulting in lowering the level of Personal Data protection,

5.1.5 ensure the confidentiality of Personal Data to which they gain access,

5.1.6 use computer and network resources only for the realization of their obligations,

5.1.7 use Internet access in a safe and responsible manner,

5.1.8 accept the fact that Internet traffic analysis is conducted by Hillwood,

5.1.9 use Hillwood e-mail to send information related to the activities of Hillwood,

5.1.10 do not store work-related information in private e-mail accounts,

5.1.11 store work-related information in the My Documents and Desktop folders, or in company-approved cloud storage applications (Hillwood Box or OneDrive accounts),

5.1.12 store private information in a location other than the one specified in section 5.1.11 and ensure that the nature and scope of such information does not infringe applicable law,

5.1.13 do not use peer to peer applications,

5.1.14 in the event of hardware failure, they immediately inform the IT department thereof without undertaking an independent repair attempt,

5.1.15 ensure the security of the workstation, in particular block the computer, enable a Password-protected screensaver or log out of the system when leaving the workstation,

5.1.16 ensure that Passwords to the system or the Application are not written down and left in easily accessible places,

5.1.17 demonstrate caution when receiving an e-mail from unknown senders,

5.1.18 process Personal Data only for the purpose and to the extent resulting from the entrusted tasks;

5.1.19 cooperate with the Data Protection Coordinator in determining the causes of the breach of Personal Data and removing the consequences of such breaches, including the prevention of their possible recurrence.

6. PERMITTED OBJECTIVES FOR THE USE OF THE IT INFRASTRUCTURE AND INFORMATION SYSTEMS

6.1 IT Infrastructure and Information Systems are the tools accessed by the Information System Users in connection with their duties and should be used solely for the performance of such duties.

6.2 Even though the Data Controller does not encourage the Information System Users to use the IT Infrastructure and Information Systems for private purposes, in exceptional circumstances, when it is justified by personal reasons, such use of the IT Infrastructure and Information Systems may be deemed acceptable, subject to the exclusions referred to in section 6.3 below. The Information System Users must be aware of the fact that the Data Controller has the right to monitor the use of the aforementioned tools. Even though the Data Controller respects the privacy as well as secrecy of private correspondence and shall not intentionally breach thereof, the Information System Users must be aware of the fact that their using of the IT Infrastructure and Information Systems for private purposes may result in the risk that the Data Controller or persons authorized thereby may have access to their private Personal Data.

6.3 In any case, the use of the IT Infrastructure and Information Systems, for private or official purposes, may not involve:

6.3.1 illicit acts, in particular the violation of the antibribery or competition protection regulations,

6.3.2 acts undertaken in violation of the Data Controller's internal policies, in particular concerning Personal Data protection;

6.3.3 acts being in conflict with the Data Controller's interests, in particular those related to the conflict of interests, competitive activity or violation of non-disclosure obligation;

6.3.4 unethical acts, in particular violation of rights and freedoms of other Personnel Members, such as mobbing, harassment or discrimination, including offensive content or other socially unacceptable behaviour;

6.3.5 acts that in the reasonable opinion might pose a threat to the Information Infrastructure and Systems' security, such as visiting adult only websites, which are often infected with viruses or downloading files from such sites.

7. OPENING, SUSPENDING AND CLOSING THE SYSTEM

7.1 Before starting to use the Information System, the Information System User must check all the IT devices as well as his/her workstation, in particular in terms of any potential Personal Data security breach.

7.2 If such Personal Data security breach is identified or suspected, the Information System User must follow the procedure provided for in the Policy.

7.3 The Information System User must position the computer screen so that to prevent it from being seen by any unauthorized persons unless it is impossible for objective reasons.

7.4 Any third party may be present near the computer only, when accompanied by an authorized person.

7.5 The Information System start procedure is as follows:

7.5.1 the User starts with entering his/her Identifier and Password in the Information System,

7.5.2 then the User opens the Application,

7.5.3 then the User starts working.

7.6 The Information System suspension procedure is as follows:

7.6.1 If the system needs to be suspended, the User should cancel all the started Personal Data operations in the system and wait until they are closed by the system.

7.6.2 Whenever the User leaves his/her workstation, he/she must not leave data Carriers unprotected.

7.6.3 Before leaving his/her workstation, the Information System User shall:

(a) wait, until password-protected screensaver is on; or

(b) block the workstation, or

(c) log out of the Information System.

7.7 The Information System closing procedure is as follows:

7.7.1 close the Application,

7.7.2 log out of the Information System,

7.7.3 turn off the computer,

7.7.4 if possible – protect the workstation from unauthorized access.

8. MANAGEMENT OF THE IT INFRASTRUCTURE

8.1 Main rules of the Information System operation:

8.1.1 persons authorized to process Personal Data shall be responsible for following the existing operational procedures,

8.1.2 Information Systems should be equipped with error detection mechanisms during routine operations.

8.2 The main rules of Personal Data storage include:

8.2.1 backing up all the data stored in the Information Systems;

8.2.2 permanently and irreversibly erasing all Personal Data from any Carriers that are decommissioned.

8.3 The invasive software protection procedure shall be as follows:

8.3.1 the User shall immediately notify his/her superior as well as the Data Protection Coordinator about any detected Viruses, and if the User has no superior – Data Protection Coordinator.

8.3.2 latest version antivirus software should be installed on all computers,

8.3.3 software that is not on the approved software list provided by Hillwood may not be used or installed.

8.4 Main rules for the Personal Data transfer and receipt:

8.4.1 Users may not use email boxes other than those assigned to them individually;

8.4.2 transfer and receipt of Personal Data or software used for Personal Data processing to and from a third party provider should be performed based on an agreement that provides for the security of such exchange.

8.4.3 All the communication within Hillwood shall be exchanged via encrypted channels using personal authentication certificates.

8.5 Personal Data protection using encryption technologies used for the information transmitted via public network should take place only with the use of algorithms or encryption tools, while the access to encryption keys should be under strict control and should be limited to a need-to-know basis.

8.6 Information System use terms:

8.6.1 Hillwood's Information Systems may only be used for the purpose of performance of duties,

8.6.2 Information System resources may only be processed as intended,

8.6.3 Information System safeguards may only be checked by authorized personnel;

8.6.4 Information Systems may provide access to resources via personal accounts assigned to individuals or service accounts with the assigned supervisor.

8.6.5 None of the Users, except for administrators appointed by the Company – shall have the access to the Information System administrative tools.

9. BACKUP COPIES

9.1 If the Company is solely responsible for the processing of Personal Data sets, such Data sets as well as the software and software tools used for processing thereof shall be stored on external data Carriers (e.g. streamers, removable disks, magnetic or optical disc drives). Backup copies made for subsequent time periods should be marked accordingly and should be stored in dedicated and properly protected rooms.

9.2 Backup should be performed regularly, as specified in Appendix 1.

9.3 IT Administrator shall be responsible for backup, as well as marking and storage of backup copies, unless the Data Controller's Management has appointed another person.

9.4 The person referred to in section 3 shall also be responsible for checking the backup copies on external data Carriers for any errors.

9.5 Backup copies should be stored in a separate room.

9.6 Damaged or obsolete backup copies shall be destroyed immediately as follows:

9.6.1 backup copies on magnetic and optical Carriers shall be destroyed by the person responsible for backup in the presence of the Data Protection Coordinator or a person appointed thereby;

9.6.2 all the data stored on magnetic and optical rewritable Carriers (e.g. CD-RW) should be deleted permanently in a way that makes it impossible to read the data, where such deletion is not possible, the Carriers should be destroyed so that to prevent data recovery,

9.6.3 data stored on recordable optical Carriers, e.g. CD-R should be deleted by complete Carrier destruction.

10. FUNCTIONALITY OF THE INFORMATION SYSTEMS USED FOR PERSONAL DATA PROTECTION BY THE DATA CONTROLLER

10.1 Servers have backup power supply (redundant power supply, power generator or UPS) to ensure safe Information System switch off, after all the system applications and software have been closed.

10.2 Information System server should be equipped with UPS with parameters sufficient to supply power until the server is safely switched off so that all the started Personal Data operations can be safely closed in case of power failure.

10.3 If any defective/damaged hardware is sent for repairs, Data Controller shall endeavour to provide replacement hardware of identical (analogical) parameters as the defective

hardware. Personal Database processing is subject to the backup procedure to prevent data loss or unintended alteration.

11. STORAGE OF PERSONAL DATA CARRIERS

11.1 Users that use Personal Data Carriers may not leave such Carriers unattended in places that can be accessed by the public and unauthorized Hillwood personnel.

11.2 Personal Data recorded on Carriers may also be stored:

11.2.1 on servers located in areas dedicated to Personal Data processing;

11.2.2 on workstations;

11.2.3 on removable electronic Carriers.

11.3 Removable data Carriers, when not used should be stored in locked drawers or cabinets or in a safe. Only authorized Hillwood personnel should have access to the Carrier storage areas.

11.4 Magnetic and optical Personal Data Carriers shall be stored for not longer than it is required for the use or potential use of the data stored thereon, in locked rooms, which may be accessed by authorized Hillwood personnel only.

11.5 Damaged or obsolete magnetic or optical Carriers shall be destroyed so that to prevent recovery of the data stored thereon by a dedicated software.

11.6 Devices, hard drives or other Carriers containing unrecoverable Personal Data should be destroyed officially so that to prevent any recovery of the information recorded thereon. Each such procedure shall be certified by a destruction report.

12. ANTIVIRUS PROTECTION

12.1 Antivirus protection is provided via antivirus software installed on workstations of the Information System Users.

12.2 Hillwood uses *CarbonBlack* antivirus software.

12.3 Antivirus software shall be regularly updated.

12.4 The following procedure shall apply in case of Virus detection:

12.4.1 disconnect all the suspected computers from all the computer networks, including wireless networks,

12.4.2 remove the Virus from the infected computer,

12.4.3 scan the network with the antivirus software,

12.4.4 connect the computer to the computer network,

12.4.5 re-scan the network with the antivirus software,

12.4.6 try to ascertain, how the Virus penetrated the company network.

12.5 If the security incident was caused by the system or software errors, the patches should be installed on all computers.

12.6 In case of suspected system or software file corruption, a new system copy should be installed.

12.7 IT Administrator shall prepare a final report with the information of all the actions undertaken, when Virus was detected.

13. PRINCIPLES OF MONITORING, CHECKUP AND MAINTENANCE OF THE INFORMATION SYSTEM

13.1 IT Administrator shall be responsible for the system check-ups, quality, maintenance and modification documentation.

13.2 All the Information System check-ups, repairs and maintenance operations performed at the place where the system is used should be done in the presence of the IT Administrator or a person appointed thereby, unless it is technically impossible or subject to significant difficulties.

13.3 If the Information System needs to be checked up, repaired or maintained elsewhere, the element, where the Personal Data are stored should be removed, if possible. Otherwise, a data processing agreement should be signed with the entity performing the repairs.

13.4 If access is required to Personal Data by the service personnel, such personnel shall sign a non-disclosure statement or data processing entrustment contract, if so required.

13.5 Software and software tools should be checked if the Application or database software is updated or if the Information System design is modified due to such repairs, maintenance or modifications.

14. DATA PROCESSING ON MOBILE DEVICES

14.1 Personal Data processed on mobile devices (laptop, tablet, mobile phone, etc.) should be sufficiently protected to ensure such data confidentiality, in particular such Data should be encrypted.

14.2 Databases of data processing systems are stored on servers in the data processing dedicated area.

14.3 Users processing Personal Data or storing temporary files with Personal Data on mobile devices should ensure the protection measures listed below:

14.3.1 device must be transported so that to minimise the risk of damage or theft,

14.3.2 mobile devices must not be left unattended in public areas,

14.3.3 mobile devices may only be transported in hand baggage,

14.3.4 computers must be transported in special computer bags to protect them from damage or destruction,

14.3.5 mobile devices may not be left unattended and in visible place in hotel rooms and should be locked in a safe, if possible,

14.3.6 using mobile devices to process Personal Data in public areas and in public transportation should be avoided,

14.3.7 it is forbidden to let unauthorized persons use mobile devices,

14.3.8 mobile computers should be blocked even if left only for a short time,

14.3.9 Personal Data recorded on the mobile device hard drive should be encrypted,

14.3.10 level of mobile computer security should be at least the same as for desktop computers,

14.3.11 protection level for mobile devices other than mobile computers should be as far as possible the same as for desktop computers,

14.3.12 mobile devices should be configured so that they are locked automatically after a specified time period,

14.3.13 at the end of work, the mobile computer screen should be closed so that the computer needs to be logged on again,

14.3.14 automatic screen saver should be activated on mobile devices after not more than 2 minutes of inactivity.

14.4 If a mobile computer is lost, damaged or stolen, the user should notify the IT Administrator immediately.

15. USE OF THE TELECOMMUNICATIONS NETWORK

15.1 Personal Data should be transmitted over network using all the required measures protecting against unauthorized access, encryption in particular (including password protection of MsWord and MsExcel files).

15.2 IT Administrator should protect the Information System from any public network threats by implementing logical security measures protecting against unauthorized access, by:

15.2.1 control of the information exchange between the Information System and public network;

15.2.2 control of any operations initiated from the public network and Information System.

15.3 The aforementioned control should be documented by performing persons.

16. RECORDING PERSONAL DATA SHARING WITH OTHER INFORMATION SYSTEM

16.1 If Personal Data is shared by the Information System used for Personal Data processing, such system should record the date, scope and the entity, with which the Personal Data was shared.

17. AREAS OF PROCESSING PERSONAL DATA

17.1 Personal Data may be processed in dedicated areas, including offices and some of the rooms, where Hillwood conducts its operations. Such rooms include, in particular:

17.1.1 offices, where the computers or servers used for the processing of Personal Data are located,

17.1.2 rooms, where non-IT resources are stored, as well as source documentation and printouts from the Information System containing Personal Data,

17.1.3 rooms, where devices, electronic data Carriers as well as Personal Data backup copies are stored.

17.2 The rooms, where Personal Data are processed, should be locked with a key in the absence of persons authorized to process Personal Data to prevent any unauthorized access.

17.3 If the devices or Carriers containing Personal Data, including sensitive data, are removed from the Personal Data processing area, they should be protected so that to ensure confidentiality, integrity and accountability of such data, which means that:

17.3.1 the access to Personal Data is protected with a password preventing unauthorized access,

17.3.2 encryption methods are used,

17.3.3 appropriate physical safeguards are used,

17.3.4 appropriate organizational safeguards are used.

17.4 Depending on threat level, the combination of the aforementioned safeguards should be used.

18. BREACH OF PERSONAL DATA PROCESSED BY HILLWOOD

18.1 Personal Data breach in Information Systems shall include, in particular:

18.1.1 unauthorized access, modification, copying or destruction/deletion of Personal Data processed in the Information System,

18.1.2 failure to protect Personal Data by allowing third party access (e.g. by leaving a copy of Personal Data, failing to block computer access, failing to monitor service personnel and other persons not authorized to access the rooms, where Personal Data is processed),

18.1.3 illegal or unintentional disclosure of Personal Data,

18.1.4 obtaining Personal Data from illegal sources,

18.1.5 detection of computer Viruses or other software posing threat to the Information System integrity,

18.1.6 making unauthorized copies of Personal Data,

18.1.7 theft of Carriers or software containing Personal Data or hardware used for the processing of Personal Data,

18.1.8 loss of Personal Data stored in the Information System on backup copies or other Carriers,

18.1.9 other situations indicating or confirming Personal Data breach in Hillwood.

18.2 The procedure applicable to the Personal Data breach in the Information System has been described in section 12 of Data Protection Policy and Data Breach Policy.

APPENDIX 1

BACKUP METHODS AND FREQUENCY

1. Backup is performed automatically by the Information System on the internal backup server.

2. Full backup copies are made weekly at a specific time. Incremental (only recently-changed data) backups are made daily at a specific time.

3. Backup copies are stored on disc space of production servers and backup server.

4. The backup copies should be stored as follows:

   (a) daily backup copies – for 14 days,

   (b) weekly backup copies – for 5 weeks,

   (c) monthly backup copies – for 36 months,

   (d) quarterly backup copies – for 5 years

   (e) yearly backup copies - for 7 years.

5. Backup copies shall be checked by IT Administrator in terms of data recovery in case of the Information System failure at least once a year.

6. In case of emergency, when IT Administrator is not present, the Data Controller's Management shall provide backup copies to another appointee.

7. Backup copy Carriers, damaged or obsolete backup Carriers shall be erased, and if it proves impossible - destroyed so that to prevent data recovery.

8. Backup copies should be destroyed in accordance with the procedure descried herein.