

## INFORMATION SECURITY POLICY

**London, 17/05/2018**

*Place, date*

### **Contents**

1. Definitions of Terms Used
2. Purpose and Scope
3. Classification of Information
4. Systems Involved in Data/ Information Processing
5. Obligations of Employees
6. Access and Protection Management
7. Security Measures
8. Prohibited Activities
9. Reporting Security Incidents

### **1. Definitions of Terms Used**

Company	<b>SINTEC UK Ltd.</b> , registration No. 5688495, legal address <b>Unit 23 Metro Centre, Britannia Way London, NW10 7PA United Kingdom</b> , who is employer of every employee employed on basis of an Employment Agreement
Direct Manager	A representative of the Company who is indicated in the Employment Agreement of respective Employee or appointed by order of the Company as direct manager of the Employee
Employee	An individual employed by the Company
Management	Board of Directors, Managing Director and/or any other person in the Company being granted managerial functions and authority
Policy	This Information Security Policy
Third Party	Individual, legal entity or other person not related to the Company

### **2. Purpose and Scope**

- 2.1. Information security system within the Company is aimed at protecting Employees, partners and customers of the Company from illegal or damaging actions by individuals, either directly or implied, knowingly or unknowingly when processing information and data which come at their disposal, as well as using certain equipment for fulfilment of their work duties.
- 2.2. The Policy shall apply on processing of information within any systems or held on any media involved in the data/ information processing within the Company, irrespective of whether data/information processing is related to internal business operations of the Company or to external relations of the Company with any third parties.
- 2.3. This Policy shall also apply on how Employees of the Company are using equipment and tools made available to them for performance of their work duties.
- 2.4. The Policy may be applicable in conjunction with any other policies, regulations, procedures and/or guidelines from time to time adopted and introduced by the Company.
- 2.5. All information security system issues and information/ data security issues not covered by this Policy shall be addressed to **gdpr@sintec.uk.com**.

### **3. Classification of Information**

- 3.1. Any information/data which becomes available to the Employees within performance of their work duties if related to Company and its operation, clients or cooperation partners, shall be deemed proprietary and confidential information of the Company thus being subject to protection in accordance with applicable laws and regulations regarding protection of confidential information, commercial/trade secrets and personal data.

3.2. In order to establish proper protection of information and data, the Company performs classification of information within the Company. Information/ data are subject to protection irrespective of whether such information has come into disposal of Employee in printed materials, any data storage devices, audio/ video materials or in any other manner.

3.3. General information classification applied within the Company:

Category	Description	Samples (including but not limited to)
Public information	Information, which could be processed and distributed within the Company or outside of it without any negative impact for the Company, any of its partners, clients and/or related parties	(a) Financial reports published to public authorities; (b) Information available in public resources or being otherwise publicly known except if it has become public due to the Employees acting in breach of information/ data security regulations
Internal information	Any information use in any manner whereof in case performed in breach of requirements of applicable laws and/ or regulations, this Policy or any other regulation adopted by the Company may harm interests of the Company, and/or any Employee, partners, clients of it	(a) Documents developed and/or prepared by any Employee, structural unit of the Company; (b) Any directories (contact, information etc.) established and/or used for business purposes of the Company; (c) Any internal working notes, memos, statements, opinions developed for business needs of the Company
Confidential information	Any information of such importance to the Company, any of its clients and/ or partners or related parties unauthorized disclosure whereof could adversely impact business, operations, reputation, status in general of the Company, its shareholders, clients and/or cooperation partners and as a consequence of such disclosure causing serious damage to any of these persons	(a) Policies, procedures, internal regulations, management decisions; (b) Information indicated to the Employee as commercial secret of the Company; (c) Other information of financial, HR, legal, marketing essence, sales procedures, plans and operations; (d) Business, product plans; (e) Personal ID data; (f) Information, which is subject to protection under confidentiality agreement each Employee signs; (g) Information, which is subject to protection under confidentiality agreements or cooperation agreements the Company has entered into within course of its business operation

#### 4. Systems Involved in Data/ Information Processing

4.1. Any information systems, including but not limited to computer equipment, any type of software, operating systems, any storage media, network accounts, electronic mail accounts, browsing systems and any other technical base and tools used in operation of the Company shall be deemed property of the Company.

4.2. Any Employee should use such technical equipment and tools with due care and attention, and only for Company business related purposes. The only exception is cases where the Company has granted to the Employee technical equipment (for instance, cell phone) explicitly permitting private use of it as well.

#### 5. Obligations of Employees

5.1. Any information/data coming into disposal of the Employee while performing his/her work duties shall be deemed and treated as confidential, treated as subject to protection according to this Policy and shall not be disclosed to any third parties until or unless the Management announces that such information has become public or otherwise has been requalified into information which is no longer subject to protection established hereby.

- 5.2. All personal data and other information by means of which an individual can be identified shall be collected and processed only if required and to the extent required for performance of work duties of the Employee, provided such activities are performed within frame of authorities granted to the Employee and in accordance with statutory requirements on protection of data (especially in accordance with requirements of Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)).
- 5.3. Any requests regarding data and/ or data processing Employee during performance of his/her work duties has received from data owners – individuals shall be immediately forwarded for further processing to the Management.
- 5.4. Each Employee must adhere to this Policy, as well as comply with requirements of applicable laws and regulations whether local, regional or international establishing requirements for information/ data processing and protection. Incompliance with the Policy shall be deemed material breach of established employment order and could lead at discretion of the Company to disciplinary sanctions or dismissal of the Employee. It could also result in an administrative or criminal liability for the Employee acting in breach.

## **6. Access and Protection Management**

- 6.1. Any devices available to Employees are accessible for them based on their work duties, responsibilities and “need to know” bases. Accessibility to any system does not imply that the Employee is authorized to view or use all information within the specific system.
- 6.2. Applied user IDs are unique and identify specific Employee. Every Employee shall be responsible for all actions associated with his/her personal ID account, therefore the primary duty is to ensure that ID of the Employee is not available to any third parties and not even to other Employees, except if the Company has established different order.
- 6.3. System security passwords shall be created with due care provided they are not easy to guess, do not include personal data, are changed on regular basis (not less than once per 3 months). Every Employee is personally liable for his/her security password compliance with this Policy and any other regulations of the Company.
- 6.4. Confidential information/data shall be approached by the Employee only if such authority is granted to the Employee by his/her Employment Agreement, and/or authorizations granted to the Employee by the Company.

## **7. Security Measures**

- 7.1. All data and information collected and processed in any form (paper, electronic etc.) shall be subject to requirements of this Policy and any statutory regulation in respect to collection, processing, protection and retention of data/ information and such documents shall be stored in safe place designated by the Company for a retention period provided for by applicable laws and/ or indicated by the Company.
- 7.2. Employees are not permitted to keep any confidential information on their devices except information which is temporarily needed for specific, work related activity. All confidential and personally identifiable information needed should be stored only in cloud storage approved by IT personnel of the Company and on the Company intranet. Any download of such files to local devices should be avoided and limited only to due necessity related with information processing for work purposes.
- 7.3. Internet access and operations performed by Employees there according to requirements of the applicable laws and regulations may be filtered and monitored by duly authorized IT personnel of the Company.
- 7.4. Any mobile, portable devices (including laptops, tablets, smartphones and other hand held computing devices), as well any cloud information storages places should be approved by IT personnel of the Company and duly secured to prevent unauthorized access.
- 7.5. Only systems and program software licensed and authorized by the Company can be installed and used on equipment and tools used within the Company. Before downloading or installing any software to devices held

and used by Employees for the purposes described in this Policy permission from the IT personnel shall be obtained.

- 7.6. In cases when Employees use home devices for access to corporate resources of the Company (e.g. CRM, e-mail, online/ cloud databases), the Employees shall be obliged to comply with requirements of this Policy equally as if they were using equipment provided by the Company. Accordingly it shall be prohibited to store any data and information related to the Company on the device; any processing of the data shall be permitted only through cloud and online storage places used by the Company.
- 7.7. At all times it shall be strictly prohibited to use public access devices (e.g. at internet cafe's, libraries etc.) unless it is critical and urgent work related necessity and Direct Manager of the Employee has provided explicit written consent for such action.
- 7.8. In case access is granted to the Employee to a files storage system of a client or cooperation partner of the Company the Employee shall be obliged to use the access tools provided by the client or partner, and follow provided guidelines on secure information/ data processing requirements (incl. use of encryption systems, passwords, data use limitations, using dedicated locations etc.).
- 7.9. Once at discretion of the Company data/ information subject to protection is no longer required for operation of the Company, such data/ information shall be deleted, all copies thereof destroyed and Employees involved in processing of respective information/ data shall be informed accordingly on their duty to delete/destroy and hand in back to the Company the information/data they no longer require for fulfilment of their work duties, and especially to deliver back to Company, delete and destroy copies in case of termination of employment of the respective Employee.
- 7.10. No information / data referred to in this Policy shall be sent, forwarded or otherwise submitted to any Third Party, unless it is necessity for accomplishment of work duties of the Employee and to the extent it is required for accomplishment of such duties. In case of forwarding and submission of data to Third Parties it shall be ensured that the data are protected and corresponding security measures have been taken.
- 7.11. Company shall audit the systems used in processing of information/ data to control ongoing compliance with this Policy and applicable statutory requirements.

## **8. Prohibited Activities**

- 8.1. Safe for exceptions specifically established, in no case and under no circumstances should any equipment, systems or tools owned by the Company, its clients or cooperation partners be used for purposes not related to work duties of the Employee or not related to business operation of the Company.
- 8.2. The following activities are strictly prohibited, with no exceptions:
  - (a) Violation of the rights of any person or company protected by intellectual property rights, including but not limited to installation, copying, distribution or storage on any Company systems or equipment of any illegal software, online platforms, any other electronic contents which is not licensed for use of the Company;
  - (b) Unauthorized copying of materials subject to copyright protection;
  - (c) Violation of the rights of any person by excessive and unnecessary collection and processing of personal data of such person;
  - (d) Accessing data, server or an account for the purpose other than conducting business operation of the Company or performance of work duties of the particular Employee;
  - (e) Exporting of software, technical information, encryption software or technology in breach of applicable international or national laws and regulations, and/or directions of the Company;
  - (f) Exporting of any data or information which is of proprietary and/ or confidential value to the Company, if such exporting is not required in the course of business operation of the Company or performance of work duties of the Employee, and/ or is in breach of internal regulations of the Company, applicable laws or regulations;

(g) Revealing Employee's account password to others and allowing use of such account by others (including but not limited to Employee family members);

(h) Making fraudulent offers of products, items or services originating from the Company account;

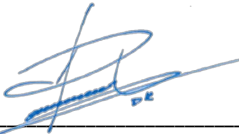
(i) Effecting security breaches or disruptions of network communication. Such security breaches include, but are not limited to, accessing data of which the Employee is not an intended recipient or logging into a server or account which the Employee is not expressly authorized to access, unless such access rights are granted to the Employee due to him/her being involved in a specific project of the Company;

(j) Using any program/script/command or sending message of any kind with intent to interfere with or disable a user session via any means.

## **9. Reporting Security Incidents**

9.1. All information/data processing security incidents or threatened incidents shall be immediately reported to Management, which accordingly shall take all measures for prevention of potential damages, elimination of the damage caused and restitution of previous security status.

9.2. If applicable, it shall be obligation of the Management to ensure further reporting on data/information security breach to authorities and individuals involved as provided for by applicable laws and regulations and/or laws of the European Union.



*Signature*

Dimitri Romaniuk, Director

*[name, surname, position of the signatory]*