ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.

INFORMATION SYSTEMS GENERAL STANDARDS AND SECURITY POLICY

6.11.2019 / Version No: 1

TABLE OF CONTENTS

ARKAS PETROL ÜRÜNLERİ VE TİCARET A.Ş.

INFORMATION SYSTEMS GENERAL STANDARDS AND SECURITY POLICY

6.11.2019 / Version No: 1

1. Purpose

Information security is comprised of 3 main elements: “confidentiality”, “integrity" and “availability”. If any of these main security elements are damaged, a corporate security weakness occurs.

- *Confidentiality*: Refers to preventing data from unauthorized access.
- *Integrity*: Refers to preventing unauthorized changes to data
- *Availability*: Refers to the availability of data to authorized persons when needed.

The purpose of this policy is to;

1.1. Ensure the security and confidentiality of all kinds of commercial and operational information and data present within the physical or electronic environments of the Data Controller,

1.2. Ensure the physical safety of all electronic information systems equipment of the Data Controller,

1.3. Ensure the efficient use of electronic information systems equipment and related service resources of the Data Controller that were procured by any means (purchasing, producing, partnering, etc.) to conduct general business activities and preventing them from being used for personal interests or malicious intentions,

1.4. Ensure that all kinds of electronic information systems equipment and the related service resources of the Data Controller that are in use are legal and licensed,

1.5. Protect the Data Controller’s corporate identity and structure, to support the development of its corporate structure,

1.6. Perform information security processes in compliance with the laws and regulations.

2. Definitions

- *Information Systems*: Electronic, magnetic, written and other platforms in which the data/information is stored, recorded, processed, transmitted and equipment, systems, personal computers (PC), servers, notebooks (laptop, notebook); smartphones, tablets, active devices, floppy disks, cartridges, CD, DVD and BD media, backup units, wired/radio communication devices, routers, hubs, switch and modems; network connections and systems, faxes, printers, photocopying devices, and all the software, programs, applications etc. connected to the systems.

- *Information Technologies Directorate (ITD)*: Refers to the internal department of the Data Controller that provides information technologies and support services to the Data Controller.

- *Information Systems Security (ISS)*: Refers to the sub-unit within the Information Technologies Directorate that is responsible for the security of information systems and that provides support services to the Data Controller.

- *Confidential/Valuable Information*: Refers to information in the possession of the Data Controller that has commercial, material or sentimental value or information that may have any potential commercial value in the future or that may give a competitive advantage; information related to the Data Controller’s business methods, work style, business volumes, finalized or ongoing projects, trade secrets; all kinds of technical or confidential information including information systems licenses, infrastructures; information/data collection, storage, transmission and access methods; information about software, programs and source codes, passwords, special

authorization parameters, electronic mail (e-mail) addresses, company telephone numbers; financial information, new business or service ideas, sales strategies, solutions, customer list and portfolios, industrial designs, brand/product names, registrations, documents, pictures, drawings, schematics, industrial properties and copyright information, logos, emblems, slogans, and information regarding all kinds of equipment, products, etc. produced and used in electronic or other kinds of platforms.

- *Service Desk*: The ITD unit that provides information systems assistance and troubleshooting to the Data Controller's employees and provides the initial point of contact for solving IT questions and problems.
- *The Law:* Refers to Personal Data Protection Law No. 6698. The purpose of this Law that was enacted on 24/3/2016 and entered into force on 7/4/2016 is to protect the fundamental rights and freedoms of persons, privacy of personal life in particular, while personal data are processed, and to set forth obligations of natural and legal persons who process personal data and procedures and principles to comply with for the same.
- *Personal Data*: Refers to any information relating to an identified or identifiable natural person; such as name, surname, date of birth and place of birth of the persons, information about the physical, family, economic and other characteristics of the person, name, telephone number, motor vehicle license plate, social security number, passport number.
- *Special Categories of Personal Data*: Refers to personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data.
- *System Devices*: Refers to equipment, hardware, software, programs and applications such as electrical and energy production and support devices, UPS, generator, etc. that allow uninterrupted operations of all information systems and data communication channels of the companies, that support the infrastructure and that has critical value, that need to be located in system rooms or in determined areas where systems rooms are not available, that can only be used/accessed by authorized employees.
- *System Access Connections/Sessions*: Connecting, logging in, accessing, etc. (domain/network login/logon, AS400 sign on, etc.) to domains, network areas, and systems, server systems using certain parameters, username/password or any similar authorized access equipment through information systems
- *Third Parties*: All official or unofficial institutions, companies, organizations, person or persons other than the Data Controller.
- *Data/Information*: All kinds of data/information that is stored, recorded, processed and transmitted in electronic, magnetic, written and other platforms, equipment, systems, personal computers (PC), servers, notebooks (laptop, notebook); smartphones, tablets, active devices, floppy disks, cartridges, CD, DVD and BD media, backup units, wired/radio communication

devices, routers, hubs, switch and modems; network connections and systems, faxes, printers, photocopying devices, and all the software, programs, applications etc. connected to the systems.

- *Data Communication Channels*: Refers to information systems that allow access to all kinds of general-purpose data/information or confidential/valuable information or transmission, copying and transfer of all these data/information via various means (wired/radio communication, Internet, telephone, GSM, e-mail, network copying, transportation to backup devices, CD, DVD, BD, etc. media, fax, modem, photocopy, printer, etc.) to platforms other than the platform in which all these data/information is located.
- *Data Controller*: ARKAS HOLDİNG A.Ş. and subsidiaries, affiliates and all companies with which they will establish and establish partnerships, regardless of partnership share rates. Means the natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data filing system.
- *Data Controllers' Contact Person (DCCP*): It refers to the natural person assigned and notified during registry by the data inventory responsible for natural and legal entities established in Turkey and by the data controller's representative for real and legal entities not established in Turkey in order to ensure communication with the Authority in relation to the obligations under the Law and secondary regulations to be issued based on this Law.

3. Scope

This policy applies to all employees of the Data Controller (includes all employment types, permanent employees, contract employees, interns, etc.), with all kinds of authority, titles and job descriptions. All employees of the Data Controller are obliged to read, understand and comply with the standards and rules set out in this policy.

4. Authorities and Responsibilities

4.1. *Responsibilities of the Managers of the Data Controller*

4.1.1. They are responsible for emphasizing the importance of the determined policies and standards to the employees working under their supervision and performing regular controls as to their applications within the scope of institutional and legal requirements.

4.1.2. They shall ensure that the employees working under their supervision understand the policies and standards and shall ensure compliance with the policies.

4.1.3. They shall help employees under their supervision to get security awareness.

4.2. *Responsibilities of the Employees of the Data Controller*

4.2.1. They are obliged to carry out the information systems operations in accordance with the determined rules and standards by receiving assistance from the Service Desk units of the ITD when necessary.

4.2.2. They shall notify the Service Desk or ISS units as soon as they come across any breaches of the related safety standards and policies.

4.3. *Responsibilities of the ISS Unit*

Information systems set the security policies and standards. They ensure the implementation of these policies and rules and perform regular controls.

4.4. *Responsibilities of the Related ITD Units*

They are obliged to know and apply the relevant safety standards and technical regulations. They provide assistance and support to the Data Controller's employees based on the determined policies and standards.

5. Rules and Application

5.1. Data/information in electronic or other platforms within the organization is the property of the Data Controller and all legal rights belong to the Data Controller.

5.2. All kinds of information systems, data communication channels, data/information, etc. of the Data Controller must only be used for business purposes.

5.3. Data Controller's employees must pay utmost attention to and comply with the principles of physical protection, access control, backup, security and confidentiality during the use of all kinds of information systems, data communication channels, data and information. Portable devices that are particularly vulnerable to the theft and loss risks should not be left unattended and their safety should be ensured.

5.4. It is essential to ensure the confidentiality of confidential/valuable information and all kinds of personal data that belong to the Data Controller. It is prohibited to transfer such valuable information and all personal data to outside of the Data Controller through any communication channels and to transfer them to third parties for any use or purpose. Additionally, special categories of personal data and personal data used in corporate processes shall not be kept in employees' homes, laptops or other personal portable devices and other platforms outside the workplace, whether electronic or physical. "Information Systems General Standards and Security Policy " published by the Data Controller shall be applied in special cases where the data/information has to be taken outside of the organization.

5.5. Employees of the Data Controller shall not bring along or use information systems that are not the property of the Data Controller at the building, office, company, etc. In particular cases when such an action is necessary, the bringing in of such equipment may only be made under the supervision of authorized employees with the notification and approval of the ITD.

5.6. Only authorized personnel within the ITD of the Data Controller may access the system rooms and the system devices where these rooms are not available. In cases which any other persons except the authorized employee have to enter the system rooms or access the system devices, the "Information Systems General Standards and Security Policy" published within the Data Controller shall be applied.

5.7. In cases which third parties are required to use the Data Controller's information systems and access all kinds of information on these systems through data communication channels, the "Information Systems General Standards and Security Policy" published within the Data Controller shall be applied.

5.8. No documents shall be left on the office desktops after working hours, confidential/valuable documents containing personal and corporate data and private project files should be kept in locked

drawers and cabinets that are part of office desks. Likewise, documents with password and username information shall never be left on or around the office desks.

5.9. The Data Controller's employees should not allow unauthorized access to the information systems they use through data communication channels. When they finish working on the information systems, they must run password-controlled screen protectors or exit the system by closing their access connection/sessions (logout/logoff, etc.).

5.10. No software, hardware or system can be copied or installed to the information systems with any data communication channels for any purpose without the ITD consent and approval. Data Controller's employees shall not modify software, hardware or system settings on any personal computers pre-set and provided by the ITD. Only the ITD User Support teams authorized for those systems shall make the necessary adjustments and changes.

5.11. All software used in the information systems within the Data Controller is licensed and legal; the ITD determines the product standards of these systems. Employees of the Data Controller should comply with the Law on Intellectual and Artistic Works no. 5846 that also covers computer programs.

5.12. Virus protection (anti-virus) programs shall be installed in personal computers or server systems and shall be constantly active. If the employees of the Data Controller find out that the virus protection program is not installed on the computers they use, that the program is not working or that the computer is infected with a virus, they should inform the Service Desk units as soon as possible.

5.13. User ID or passwords are personal and should not be shared with anyone. Our employees are responsible for all the corporate damages that may occur due to misconducts regarding user ID or passwords, including unauthorized access and usage. In cases where the security of the user ID or password is suspicious, the passwords should be changed and the Service Desk unit should immediately be contacted. Data Controller employees should read the "Security Standards to be Complied within the Selection and Usage of Passwords" document published by the ITD of the Data Controller for the usage of all user names, passwords, authorization systems, etc. in information systems and select and use passwords in compliance with all the rules specified in that document.

5.14. Confidential/valuable data and personal data shall not be shared and transmitted unsafely (unencrypted) through the network. Data Controller's employees can get support from our Service Desk unit for the appropriate method and policy to be used in data and information encryption for this purpose. Likewise, in cases where confidential/valuable data and personal data should be shared with another employee within the company, internal correspondence envelopes should only be sent to the data subject as "Confidential".

5.15. Apart from the internet service provided by the Data Controller within the organization, alternative internet services shall not be used. Data Controller's employees shall request authorized Internet access or any other internal and external Internet access in accordance with the relevant ITD policies and standards published by the Data Controller.

5.16. The Internet should only be used to access relevant legal, official, corporate websites within the scope of company legislation, business-related research/development, information collection, needs and purposes. Company devices shall be centrally controlled by ITD experts for safety when deemed necessary.

5.17. Data Controller employees shall use company e-mail systems, addresses, and e-mail boxes for business purposes only. E-mails containing insults, threats, swearing, political messages, slogans, propaganda, etc. shall not be sent to any employees or third parties by using the company e-mail addresses; company e-mail systems and addresses cannot be used in illegal transactions that will violate corporate company policies, rules or the laws of the country.

5.18. The Data Controller's employees shall not open any e-mails from addresses they do not recognize, e-mails whose attachments, subjects or contents are suspicious or vague, shall not forward e-mails of those kinds to any other address and shall notify the Service Desk units as soon as possible. Similarly, if the Data Controller's employees receive a virus notification, warning or news from any source (e-mail, media, Internet etc.), the Data Controller's employees must not share this information with any third parties or colleagues and shall transfer it to the Service Desk.

5.19. Memberships to all kinds of list services (social media, mailing list, newsgroup) or similar common electronic mail systems and distribution groups for business purposes must be approved by the ITD via Service Desk units.

5.20. In accordance with Law No. 5651 on Regulating Broadcasting in The Internet and Fighting Against Crimes Committed through Internet Broadcasting, all internet access and e-mail usages of the Data Controller's employees in the information security control systems of the Data Controller are recorded and monitored.

5.21. In order to protect the data owned by the Data Controller, additional security measures shall be taken for the employees that are to access to the corporate resources through data communication channels from outside the company. In these cases, the ITD specialists must conduct the necessary controls (improvement, regulation, encryption and malware prevention) in the information systems used by the employees to keep the information systems equipment accessible and working throughout the access to the corporate resources.

5.22. Users' access rights to Data Controller's corporate system resources are regulated according to business requirements. Data Controller's employees are obliged to notify the Service Desk unit as soon as they detect possible non-compliances by them or their colleagues such as access authorization sharing or exceeding access authorization limits.

5.23. Common areas and electronic mail systems are not suitable for the archive storage of personal data. The Data Controller reserves the right to remove any data, systems, and materials that may be offensive or in violation of the law from its information systems and to initiate related official proceedings.

5.24. It is prohibited to use information systems and equipment and cloud storage and messaging services (Dropbox, Gdrive, Onedrive, Whatsapp, Hangouts, Box, etc.) for non-work related purposes within the Data Controller's company. It is the ITD units' responsibility to determine and put into service corporate practices by considering business priorities for such requirements.

5.25. Our company complies with the principles of legal regulations and ensures lawfulness and fairness when processing personal data. Data Controller; handles personal data in a manner that is conducive to achieving the specified purposes and avoids the processing of personal data that is not relevant or needed in achieving the purpose. In this context, it takes into account proportionality requirements

and does not use personal data other than for the purpose of processing. For this reason, our employees should not store and use their personal data and special categories of personal data that have not been requested from them by the Data Controller's administrative and business units in their corporate resources. All personal data (except those duly disclosed and explicitly consented by the data controller) that is not related to the work and intended for personal/private use should not be kept in e-mail boxes, instant messaging software, office documents, portable computers and common areas allocated by the data controller. Additionally, employees are obliged to ensure that all personal data they process is kept securely. Personal Data shall not be shared, disclosed orally, in writing or by other means to any unauthorized third party, whether by accident or otherwise. Any situation contrary to the principles stated in the article such as unauthorized sharing of personal data should be immediately notified to the Data Controllers' Contact Person.

5.26. In case of the termination of his/her relationship with the organization; every employee shall be obliged to return all confidential/valuable information, data/information owned by the Data Controller and all information systems in which they are kept or recorded and written to the Data Controller within maximum 1 business day following the date of termination. Each employee dismissed or voluntarily resigned is liable for complying with Articles 5.1 and 5.4 of this Policy indefinitely from the date of termination of his/her relationship with the Data Controller.