Information Security Policy

IGDP_P5 VERSION 1.00

Aladdin Middle East Limited – Turkey Branch Office

Information Security Policy

1. Purpose:

Information plays a fundamental role in supporting all activities of the Aladdin Middle East Limited – Turkey Branch Office. (hereinafter referred as the "Company" or "AME Turkey") Properly securing all information that Company processes is essential to the success of its economic and administrative activities. This is to be achieved through managing the three essential attributes of information security: confidentiality, integrity and availability, which are the essential components of Company's information assets.

The objectives of this policy are to:

1.1. to ensure effective and adequate protection of all of the Company's information assets against loss, misuse or abuse;

1.2. make all users aware of this policy and all associated policies, codes of practice and guidelines;

1.3. make all users aware of the relevant applicable Turkish legislation, and their responsibilities in regard to these;

1.4. create an awareness that appropriate security measures must be implemented across AME Turkey as part of the effective operation and support of information security;

1.5. make all users understand their responsibilities for protecting the confidentiality, integrity and availability of the data they handle.

This Policy should be read in conjunction with the AME Turkey's Data Protection Policy and associated Directives, which provide more detailed guidance on protection of personal data.

2. SCOPE:

The provisions of this policy aims to install code of conduct with a view to protection of electronic information assets used through Company's economic activities and related logistics, accounting, finance, quality insurance, purchase, human resources, legal affairs, marketing, internal audits and information processing activities and information security measures we use in order to ensure that we gather, process, detain personal data in a lawful manner and information assets are kept safe from unlawful access and data breaches.

2.1. All Company staff and other authorised third parties including guests and representatives of Company's business associates, who may have access to information held by or on behalf of the Company, must adhere to the AME Turkey's Information Security Policy and its associated Codes of Practice. The scope of the policy covers aforementioned individuals' use of Company-owned/leased/rented and

on-loan facilities, and all third party systems, owned/leased/rented/on-loan, when connected to the Company network directly or indirectly, to all Company-owned/licensed data and software, be they on Company or on third party systems, and to all data and software provided to Company by sponsors or external agencies.

2.2. This Policy applies to all data held by the Company whether in electronic or physical format including, by way of example and without limitation:

- electronic data stored on and processed by fixed and portable computers and storage devices;
- data transmitted on networks;
- information sent by fax or similar transfer methods;
- all paper records;
- microfiche, visual and photographic materials including slides and CCTV; spoken, including face-to-face, voicemail and recorded conversation.

2.3. The data types held by the Company can broadly be classified as personal data and non-personal data:

- personal data is treated in accordance with the AME Turkey's Data Protection Policy and is afforded the highest standard of protection;
- non-personal data can include following categories of information:
  i. sensitive organisational data such as commercially sensitive planning data, research data, data protected by confidentiality agreements or legally privileged information – all of these categories of data are also afforded a high level of protection; and
  ii. other organisational data that is either already made public (e.g. on the Company's corporate website) or may be disclosed to the public (e.g. pursuant to a request under the Freedom of Information Act-Law No. 4982) – such data must be accurate, must be kept up-to-date and must be protected from destruction and unauthorised interference.

2.4. The provisions of this Policy apply throughout the lifecycle of all information from creation, collection, storage, and use to disposal.

2.5. Although the use of social media resources by Company staff members is unrestricted and not centrally moderated, the Company requires its members to ensure they respect this policy and cause no damage to the Company's corporate reputation.

3. RESPONSIBILITIES and POWERS:

The key roles and responsibilities at the Company with respect to information governance are set out in the AME Turkey's Information Governance Policy Framework. Of particular importance for compliance with this policy are:

3.1. Heads of Departments and Heads of Divisions

Head of Departments and Heads of Divisions are responsible that staff members and other authorised individuals within their department or division are informed, and comply with this policy, particularly rules and modalities prescribed in section 11: Conditions of Use of IT Resources. They are also responsible that all information assets held by their departments or divisions are included in the Company's Information Asset Register and an Information Asset Owner is assigned for every information asset.

3.2. Information Asset Owners

Information asset owners are the assigned owners of Company information assets as listed in the Company's Information Asset Register. They are responsible for assessing information security and privacy risks annually pursuant to the "Directive on Data Privacy Impact Assessment" for their assets and implementing appropriate measures accordingly.

3.3. Staff and authorised third parties

All Company staff and authorised third parties must adhere to this Policy and associated Codes of Practice. Compliance with the policy forms part of the Core Terms and Conditions of Service for Company staff members. Section 11 of this policy, "Conditions of Use of IT Resources (Acceptable Use Policy)" shall be displayed and must be accepted by all staff and authorised third parties before they can start using their Company user name and password. Any actual, or suspected, information security incidents (such as accidental exposure or loss, unauthorised access, computer virus, malicious software) must be reported to the IT Department immediately. Concerned individuals may contact any senior members of AME Turkey or IT Department directly.

3.4. Chief of IT Department

Chief of IT Department is responsible for overseeing IT Department's resources to manage day-to-day information security activities. The Chief of IT Department may decide to audit systems to identify and mitigate risks, or to make inaccessible/remove any unsafe user/login names, data and/or programs on the system from the network.

4. COMPLIANCE WITH LEGISLATION

4.1. AME Turkey has an obligation to abide by all Turkish legislation and relevant regulations. Of particular importance in this respect are Law No. 5651 on the Regulation of Internet Broadcasts and Prevention of Crimes Committed through Such Broadcasts, Law No 6698 on Protection of Personal Data and Network and Information Security Regulation in Electronic Communication Sector.

4.2. The requirement for compliance devolves to all users, who may be held personally responsible for any breach of the legislation. Failure of an individual member of staff to comply with this policy, or with any legislation, may lead to the instigation of the relevant disciplinary procedures as set out in the Company's labour contract employment terms and condition and staff policies. Failure of a contractor to comply

could lead to the termination of a contract. In certain circumstances, legal action may be taken.

5. COMPANY'S INFORMATION ASSET REGISTER AND DATA PRIVACY IMPACT ASSESSMENT

5.1. The Company maintains an Information Asset Register that contains the details of information assets used in AME Turkey. It is the responsibility of Heads of Departments and Divisions to assign Information Asset Owners for every information asset kept by their departments and record these in the Information Asset Register

5.2. A data privacy impact assessment must be carried out for all existing information assets annually. A data privacy impact assessment must also be carried out for all new information assets at the time of inception. For the ones identified as containing sensitive data, measures to mitigate those risks must be agreed, implemented and also included in the asset register. It is the responsibility of the Heads of Departments and Divisions to ensure that Information Asset Owners review their Information Assets annually. For further information, refer to "Directive on Data Privacy Impact Assessment".

6. CONDITIONS FOR MONITORING ELECTRONIC COMMUNICATIONS

In accordance with the Article 6 of the Law No. 5651 on the Regulation of Internet Broadcasts and Prevention of Crimes Committed through Such Broadcasts, regarding blocking access to criminal content and retaining access records entitled "Obligations of access providers", the Company will exercise its right to intercept and monitor electronic communications received by and sent from the Company for the purposes permitted under the law and relevant regulations. The purposes cover, but are not limited to, monitoring for criminal or unauthorised use, viruses, threats to the system, e.g. hacking and denial of service attacks, ensuring the effectiveness of its operations and compliance with Company policies and regulations. The monitoring process will be carried out in accordance with "Directive on Inspection of Electronic Communications and Data".

7. INFORMATION SECURITY INCIDENTS

7.1. Any user suspecting that there has been, or is likely to be an information security incident, such as a breach of confidentiality, availability, integrity of information, or misuse of an information asset, should inform the IT Department's Support Desk immediately. You may also contact any senior members of AME Turkey directly if you prefer to do so. The General Manager or, if not available, the Chief of IT Department, has the authority to take whatever action is deemed necessary to protect the Company against breaches of security.

7.2. If the incident involves accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, you should report it

immediately by completing a notification of data security breach form and sending it to:

Data Protection Liaison Officer:
ALADDİN MİDDLE EAST LİMİTED ŞİRKETİ - TÜRKİYE ANKARA ŞUBESİ
Telephone: + 90 312 427 90 20
Fax: + 90 312 427 90 25
E-mail: kvkk@ame.com.tr

7.3. In the event of a suspected or actual information security incident or an unacceptable network event, the Chief of IT Department may decide to take any immediate action necessary to remedy the situation. This may include blocking access by users to systems and examination of any devices connected to the network.

7.4. Failure to report an information security incident or data breach may lead to disciplinary action being taken. If you are in any doubt regarding whether to report an incident, you should seek advice from Chief of IT Department or the Company's Data Protection Liaison Officer.

8. SECURITY EDUCATION AND TRAINING

8.1. New users of IT facilities, staff, staffs and approved third parties, should be instructed on the Company policies and Codes of Practice relating to information security. They should also be given training on the procedures relating to the security requirements of the particular work they are to undertake and on the correct use of the Company's IT assets in general before access to IT services is granted. It is the responsibility of managers that their staff are suitably trained, and to maintain training records. They should be made aware in particular of this policy including the reporting procedures in section 7.

8.2. All new staff of the Company are expected to complete the Company's online security awareness training and a data protection e-learning course. This training is expected to become mandatory for all Company staff members in the near future.

9. SECURITY CONSIDERATIONS FOR EMPLOYMENT

9.1. Security roles and responsibilities, as laid down in this Policy and related Codes of Practice, should be included in job descriptions, where appropriate. These should include any general responsibilities for implementing the security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of particular security processes or activities.

9.2. Applications for employment or changes of role may require screening and re-evaluation of Department of Human Resources.

9.3. Agency staff and approved third party users (such as service providers and business partners) of Company information systems will be required to sign a confidentiality or

non-disclosure agreement as part of their contract as well as a data processing agreement/addendum where they will have access to Company personal data.

10. PROTECTING SENSITIVE DATA

10.1. It is essential that the Company protects sensitive data with enhanced security measures.

10.2. Sensitive data must not be stored on or communicated through services which are not provided by the Company such as personal email (Gmail, Hotmail etc…) or web-based 'cloud' storage services (e.g. Google Apps, Dropbox).

10.3. Databases and computers containing sensitive data must be encrypted and require users to input credentials to access the data. Where possible, data should be anonymised or pseudonymised to remove personal identifiers, especially where health data of staff members is considered.

10.4. All Company devices must be securely wiped before being disposed of.

10.5. Data files must be encrypted both at rest and in transit.

11. CONDITIONS OF USE OF IT RESOURCES (ACCEPTABLE USE POLICY)

Any person using Company IT resources (referred to as a "user") agrees and accepts that:

11.1. Company IT resources are all hardware, software, services and resources made available for the corporate business. They include all computer networks, wired or wireless, computers, printers, mobile devices, storage, audio visual systems, and associated information services including Cloud services

11.2. Every user must understand and abide by the advice provided, he/she must enrol and complete the Company's Information Security Awareness training, read and sign Information Security Awareness Declaration;

11.3. use of Company's IT resources, and their use to access third party IT resources, must be for the purpose of Company's research, training, associated administration or other authorised use. No private commercial work is permitted without prior authorisation;

11.4. Company business should be conducted only on information services provided by the AME Turkey. Using third party information services to carry out Company business puts Company data at risk and therefore is not allowed except with sufficient justification. For example, corporate e-mail and cloud service should be used instead of instead of Dropbox, One Drive, Gmail, Hotmail, etc;

11.5. reasonable personal use of Company IT resources is permitted provided such use does not disrupt the conduct of Company business or other users. Recreational use of the corporate Wi-Fi network is also permitted, subject to these conditions;

11.6. it is not permitted to connect active network devices such as network switches, hubs, wireless access points and routers to the Company network. All IP addresses will be allocated and administered only by IT Department;

11.7. Staff members may not grant access to Company computing services to third party staff or visitors except where expressly permitted to do so in writing.

11.8. when using Company IT resources, the user must comply with the Company's Information Security Policy including this Acceptable Use Policy, and all relevant statutory and other provisions, regulations. Specifically, but not exclusively, the user must comply with following provisions:

11.8.1. not disclose to others their Company password and must understand and abide by "Directive on Principles and Code of Conduct for User Passwords";

11.8.2. not access or attempt to access IT resources at Company premises or elsewhere for which permission has not been granted or facilitate such unauthorised access by others;

11.8.3. not use or produce materials or resources to facilitate unauthorised corruption, changes, malfunction or access to any IT resources at the Company or elsewhere, e.g. port scanning;

11.8.4. not display, store, receive or transmit images or text which could be considered offensive or which is likely to bring the AME Turkey into disrepute, e.g. material of a pornographic, paedophilic, sexist, racist, libellous, threatening, defamatory, illegal, discriminatory, or terrorist nature;

11.8.5. not forge email signatures and/or headers, initiate and/or forward 'chain' or 'junk' or 'harassing' email, must not impersonate others in electronic communication and generate junk or offensive communications and must understand and abide by "Directive on Principles and Code of Conduct for Electronic Messaging";

11.8.6. ensure all mobile devices they access Company resources with are encrypted by an appropriate encryption software, and pin or password protected;

11.8.7. respect the copyright of all material and software made available by the Company and third parties and not use, download, copy, store or supply copyrighted materials including software and retrieved data other than with the permission of the copyright holder or under the terms of the licence held by the Company

11.8.8. when holding data about living individuals, abide by the Company's Data Protection Policy, to process information (that is, collect, use, share and dispose of) in accordance with the Principles of the data protection legislation.

11.8.9. be aware that all information assets created/owned/stored by the user on or connected to Company IT resources may, in the instance of suspected wrong doing, be subjected to inspection by Company or by statutory authorities. Should the information be encrypted the user shall be required to and must provide the decryption key;

11.8.10. establish what the terms of the licence are for any material and software which he/she uses through any platform and must not breach such licences.

11.9. As provided by the Article 6 of the Law No. 5651 on the Regulation of Internet Broadcasts and Prevention of Crimes Committed through Such Broadcasts, regarding blocking access to criminal content and retaining access records entitled "Obligations of access providers", the Company will exercise its right to intercept and monitor electronic communications received by and sent from the Company for the purposes permitted under the law and relevant regulations. The implementation procedures of

these measures will be regulated by the Directive on Inspection of Electronic Communications and Data

11.10. In the event of a suspected or actual information security incident or an unacceptable network event, the Chief of IT Department may decide to take any action necessary to remedy the situation. This may include blocking access by users to systems and examination of any devices connected to the network.

11.11. In the event of further examination required, IT Department may take action to examine any systems on the Company network by express permission from the General Manager.

11.12. Other than as per any applicable statutory obligation, the AME Turkey will not be liable for any loss, damage or inconvenience arising directly or indirectly from the use of, or prevention of use of, any IT resource provided and/or managed by the Company.

11.13. Whilst the Company takes appropriate security measures against unauthorised access to, alteration, disclosure, destruction or accidental loss of personal and other data it cannot and does not give any warranties or undertakings to the user about security, confidentiality or integrity of data.

11.14. Users' name, address, photograph, status, e-mail name, login name, alias, company ID Cart and other related information will be stored in computerised form for use for administrative and other purposes e.g. monitoring system usage.

11.15. Aforementioned conditions apply to non-Company owned equipment e.g. personal Laptops, home PCs when connected to the Company network, directly and/or via the VPN, for the duration that the equipment is using the Company's network.

11.16. Breach of these conditions may lead to corporate disciplinary procedures being invoked, with penalties which could include suspension from the use of all Company IT resources for extended periods and/or fines. Serious cases may lead to expulsion or dismissal from the Company and may involve civil or criminal action being taken against the user.

11.17. All guests using Company IT facilities and/or the Company internet connection must be known to a member of Company as their sponsor. Sponsors must be able to identify and take responsibility for the actions of their individual guests.