CONDITIONS OF USE OF IT RESOURCES (ACCEPTABLE USE POLICY)

IGDP_P6 VERSION 1.00

Aladdin Middle East Limited – Turkey Branch Office

CONDITIONS OF USE OF IT RESOURCES (ACCEPTABLE USE POLICY)

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

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

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

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 authorized use. No private commercial work is permitted without prior authorization;

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.;

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;

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;

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.

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:

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";

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 unauthorized access by others;

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

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, pedophilic, sexist, racist, libelous, threatening, defamatory, illegal, discriminatory, or terrorist nature;

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”;

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

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 license held by the Company

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.

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;

8.10. establish what the terms of the license are for any material and software which he/she uses through any platform and must not breach such licenses.

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

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. 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.

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.

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.

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.

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.

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.

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.