

<p>Legate Group Limited IT Security Policy 30 September 2018</p>
--

1. Introduction

This document sets out the measures to be taken by all staff, contractors, agents and those appointed to act on behalf of Legate Group Limited, hereafter referred to as (the “Company”) and by the Company as a whole in order to protect the Company’s computer systems, devices, infrastructure, computing environment and any and all other relevant equipment (collectively, “IT Systems”) from damage and threats whether internal, external, deliberate or accidental.

2. Key Principles

- 2.1 All IT Systems are to be protected against unauthorised access.
- 2.2 All IT Systems are to be used only in compliance with the relevant Company policies.
- 2.3 All data stored on Company IT Systems are managed securely in compliance with all relevant parts of the Data Protection Act 2018 and all other laws current and future governing data protection whether now or in the future in force.
- 2.4 All employees, agents and those appointed to act on behalf of the Company and any third parties authorised to use the IT Systems including, but not limited to, contractors and sub-contractors (collectively, “Users”), must ensure that they are familiar with this Policy and must adhere to and comply with it at all times.
- 2.5 All line managers must ensure that all Users under their control and direction must adhere to and comply with this Policy at all times as required under paragraph 2.4.
- 2.6 All IT Systems are to be installed, maintained, serviced, by the Company’s Director or by such third party/parties as he may from time to time authorise.
- 2.7 The responsibility for the security and integrity of all IT Systems and the data stored thereon (including, but not limited to, the security, integrity and confidentiality of that data) lies with the Company’s Director unless expressly stated otherwise. In cases where cloud based, or remote services are utilised the Company’s Director will appoint those respective parties to investigate potential breaches and feedback accordingly.
- 2.8 All breaches of security pertaining to the IT Systems or any data stored thereon shall be reported and subsequently investigated by the Company’s Director.
- 2.9 All Users must report any and all security concerns relating to the IT Systems or to the data stored thereon immediately to the Company’s Director.

3. IT Services Responsibilities

- 3.1 The Company’s Director, shall be responsible for the following:
 - a) ensuring that all IT Systems are assessed and deemed suitable for compliance with the Company security requirements;

- b) ensuring that IT security standards within the Company are effectively implemented and regularly reviewed; and
- c) ensuring that all Users are kept aware of the requirements of this Policy and of all related legislation, regulations and other relevant rules whether now or in the future in force including, but not limited to, the Data Protection Act 1998 and the Computer Misuse Act 1990.

3.2 The Managing Director shall be responsible for the following:

- a) assisting all Users in understanding and complying with this Policy;
- b) providing all Users with appropriate support and training in IT security matters and use of IT Systems;
- c) ensuring that all Users are granted levels of access to IT Systems that are appropriate for each User, taking into account their job role, responsibilities and any special security requirements;
- d) receiving and handling all reports relating to IT security matters and taking appropriate action in response;
- e) taking proactive action, where possible, to establish and implement IT security procedures and raise User awareness;
- f) ensuring that regular backups are taken of all data stored within the IT Systems at intervals no less than 48 hours and that such backups are stored at a suitable location off the Company premises.

4. Users' Responsibilities

- 4.1 All Users must comply with all relevant parts of this Policy at all times when using the IT Systems.
- 4.2 All Users must use the IT Systems only within the bounds of UK law and must not use the IT Systems for any purpose or activity which is likely to contravene any UK law whether now or in the future in force.
- 4.3 Users must immediately inform the Managing Director of any and all security concerns relating to the IT Systems.
- 4.4 Users must immediately inform the Managing Director of any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems.
- 4.5 Any and all deliberate or negligent breaches of this Policy by Users will be handled as appropriate under the Company's disciplinary procedures.

5. Software Security Measures

- 5.1 All software in use on the IT Systems (including, but not limited to, operating systems and individual software applications) will be kept up-to-date and any and all relevant software updates, patches, fixes and other intermediate releases will be applied at the sole discretion of the Managing Director.
- 5.2 Where any security flaw is identified in any software that flaw will be either fixed immediately or the software may be withdrawn from the IT Systems until such time as the security flaw can be effectively remedied.
- 5.3 No Users may install any software of their own, whether that software is supplied on physical media (e.g. DVD-Rom) or whether it is downloaded, without the approval of the Company.

- 5.4 All software will be installed by an approved supplier unless an individual User is given written permission to do so by the him. Such written permission must clearly state which software may be installed and onto which computer(s) or device(s) it may be installed.

6. Anti-Virus Security Measures

- 6.1 IT Systems (including all computers and routers) will be protected with suitable anti-virus, firewall and internet security software. All such anti-virus, firewall and internet security software will be kept up-to-date with the latest software updates and definitions.
- 6.2 All systems protected by anti-virus software are subject to constant monitoring.
- 6.3 The Company does not permit the use of storage media (e.g. USB memory sticks or disks of any kind) on its systems.
- 6.4 All files being sent to third parties outside of the Company by email is scanned for malicious software via Microsoft Office 365 in-built security measures.
- 6.5 Where any virus is detected by a User this must be reported immediately (this rule shall apply even where the anti-virus software automatically fixes the problem). The Company shall promptly take any and all necessary action to remedy the problem. In limited circumstances this may involve the temporary removal of the affected computer or device. Wherever possible a suitable replacement computer or device will be provided to limit disruption to the User.
- 6.6 Where any User deliberately introduces any malicious software or virus to the IT Systems this will constitute a criminal offence under the Computer Misuse Act 1990 and will be handled as appropriate under the Company's disciplinary procedures.

7. Hardware Security Measures

- 7.1 Wherever practical, IT Systems will be located in rooms which may be securely locked when not in use or, in appropriate cases, at all times whether in use or not (with authorised Users being granted access by means of a key, smart card, door code or similar). Where access to such locations is restricted, Users must not allow any unauthorised individual access to such locations for any reason.
- 7.2 All IT Systems not intended for normal use by Users (including, but not limited to, servers, networking equipment and network infrastructure) shall be located, wherever possible and practical, in secured, climate-controlled rooms and/or in locked cabinets which may be accessed only by the Managing Director,
- 7.3 No Users shall have access to any IT Systems not intended for normal use by Users (including such devices mentioned above) without the express permission of the Managing Director. Under normal circumstances whenever a problem with such IT Systems is identified by a User, that problem must be reported to him. Under no circumstances should a User attempt to rectify any such problems without the express permission (and, in most cases, instruction and/or supervision) of the Company's Director.
- 7.4 All hardware containing personal or confidential information must be subject to hardware hardening to include data encryption as a minimum.
- 7.5 All non-mobile devices (including, but not limited to, desktop computers, workstations and monitors) shall, wherever possible and practical, be physically secured in place with a suitable locking mechanism. Where the

design of the hardware allows, computer cases shall be locked to prevent tampering with or theft of internal components.

- 7.6 All mobile devices (including, but not limited to, laptops, netbooks, tablets, PDAs and mobile telephones) provided by the Company should always be transported securely and handled with care. In circumstances where such mobile devices are to be left unattended they should be placed inside a lockable case or other suitable container. Users should make all reasonable efforts to avoid such mobile devices from being left unattended at any location other than their private homes or the Company premises. If any such mobile device is to be left in a vehicle it must be stored out of sight and never left overnight.
- 7.7 The Company shall maintain a complete asset register of all IT Systems.

8. **Access Security**

- 8.1 All IT Systems (and in particular mobile devices including, but not limited to, laptops, netbooks, tablets, PDAs and mobile telephones) shall be protected with a secure password or such other form of secure log-in system as the Company may deem appropriate.
- 8.2 All passwords must, where the software, computer or device allows and where a perceived risk is present:
 - 8.2.1 be at least 10 characters long;
 - 8.2.2 contain a combination of upper and lower-case letters, numbers and symbols;
 - 8.2.3 be changed at least every 90 days;
 - 8.2.4 not be re-used within 12 months.
 - 8.2.5 not be common, obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events or places etc.); and
 - 8.2.6 be created by individual Users.
- 8.3 Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone including the Managing Director. No User will be legitimately asked for their password by anyone at any time and any such request should be refused. If a User has reason to believe that another individual has obtained their password, they should change their password immediately and report the suspected breach of security to the Company's Director.
- 8.4 If a User forgets their password, this should be reported to the Managing Director. He will take the necessary steps to restore the User's access to the IT Systems which may include the issuing of a temporary password which may be fully or partially known to him. A new password must be set up by the User immediately upon the restoration of access to the IT Systems.
- 8.5 All IT Systems with displays and user input devices (e.g. mouse, keyboard, touchscreen etc.) shall be protected, where possible, with a password protected screensaver that will activate after 20 minutes of inactivity. This time period cannot be changed by Users and Users may not disable the screensaver. Activation of the screensaver will not interrupt or disrupt any other activities taking place on the computer (e.g. data processing).
- 8.6 Users may not use any software which may allow outside parties to access the IT Systems without the express consent of the IT Managing Director. Any

such software must be reasonably required by the User for the performance of their job role and must be fully inspected and cleared by the Managing Director,

- 8.7 Users may connect their own devices (including, but not limited to, mobile telephones, tablets and laptops) to the Company network subject to the approval of the Director. Any and all instructions and requirements provided by the him governing the use of Users' own devices when connected to the Company network must be followed at all times. Users' use of their own devices shall be subject to, and governed by, all relevant Company Policies (including, but not limited to, this Policy) while those devices are connected to the Company network or to any other part of the IT Systems. The Managing Director shall reserve the right to request the immediate disconnection of any such devices without notice.

9. **Network Security**

The Company's information systems will be available when needed and can be accessed only by legitimate Users. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, the Company will undertake the following: -

- 9.1 Protect all hardware, software and information assets under its control.
- 9.2 The Company will comply with other laws and legislation as appropriate.

10. **Data Protection**

- 10.1 All personal data (as defined in the Data Protection Act 2018) collected, held and processed by the Company will be collected, held and processed strictly in accordance with the eight Data Protection Principles of the Data Protection Act 2018, the provisions of the Data Protection Act 2018 and the Company's Data Protection Policy.
- 10.2 All Users handling data for and on behalf of the Company shall be subject to, and must comply with, the provisions of the Company's Data Protection Policy.

11. **Internet and Email Use**

- 11.1 All Users shall be subject to, and must comply with, the provisions of the Company's Communications, Email and Internet Policy when using the IT Systems.
- 11.2 Where provisions in this Policy require any additional steps to be taken to ensure IT security when using the internet or email over and above the requirements imposed by the Communications, Email and Internet Policy, Users must take such steps as required.

12. **Reporting IT Security Breaches**

- 12.1 All concerns, questions, suspected breaches or known breaches shall be referred immediately to the Director.
- 12.2 Upon receiving a question or notification of a breach, he shall, within 24 hours assess the issue including, but not limited to, the level of risk associated therewith, and shall take any and all such steps deemed necessary to respond to the issue.

12.3 Under no circumstances should a User attempt to resolve an IT security breach on their own without first consulting the Director. Users may only attempt to resolve IT security breaches under the instruction of, and with the express permission of, the Company.

12.4 The Company will notify the client(s) within 48 hours of a security breach.

12.5 All IT security breaches, whether remedied or not shall be fully documented.

13. Implementation of Policy

This Policy shall be deemed effective as of 01/10/2017. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

Name: Anthony Paul Clarke

Position: Director

Date: 02/10/2017

Version Control:

Version	Date	Date Approved	Next Review Date
V1	30/09/2014	01/10/2014	30/09/2017
V2	01/10/2017	02/10/2017	30/09/2019
V3	26/09/2018	26/09/2018	30/09/2019
V4	06/11/2018	06/11/2018	30/09/2019