Legate Group Limited

IT SECURITY POLICY

Revision History

Version	*Revision Date*	*Revised By*	*Section Revised*
V1	30/09/2014	T.Clarke	Whole Document
V2	01/10/2017	T.Clarke	Whole Document
V3	26/09/2018	T.Clarke	Whole Document
V4	30/09/2020	T.Clarke	Whole Document
V5	20/10/2021	T.Clarke	Access Security
V6	05/08/2022	M.McCarthy	Access Security

Document Control

Document Owner:	***Next Review Date:***	***Version:***	***Unit:***
T. Clarke	***19/10/2022***	***5***	***InfoSec***
Latest Review Comments:			

1. TITLE

IT Security Policy

2. POLICY STATEMENT

Legate Group (the "Company") is a commercial investigation company and operates as a small business. As such the Company's policy is designed to be proportionate to the risks and business size. The Company is committed to protecting the Company's computer systems and the information that is contained on it.

3. PURPOSE

This document sets out the measures to be taken by all staff, contractors, agents and those appointed to act on behalf of 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.

4. KEY PRINCIPLES

All IT Systems are to be protected against unauthorised access and are to be used only in compliance with the relevant Company policies.

All data stored on Company IT Systems will be managed securely in compliance with all relevant parts of the Data Protection Act 2018 and all other laws.

All those that are 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.

All IT Systems are to be installed, maintained, serviced, by the Company's Director or by such qualified third party/parties as he may from time to time authorise.

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.

All breaches of security or security concerns pertaining to the IT Systems or any data stored thereon shall be reported and subsequently investigated by the Company's Director or other specialist company that the Company's Director appoints.

5. IT SERVICE RESPONSIBILITES

The Company's Director, shall be responsible for ensuring that: -

All IT Systems are assessed and deemed suitable for compliance with the Company security requirements;

IT security standards within the Company are effectively implemented and regularly reviewed;

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 2018 and the Computer Misuse Act 1990;

Assisting users in understanding and complying with this Policy;

Users are provided with appropriate support and training in IT security matters and use of IT Systems;

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;

The receipt and handling all reports relating to IT security matters and taking appropriate action in response;

Proactive action is taken, where possible, to establish and implement IT security procedures and raise User awareness;

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.

6. USER'S RESPONSIBILITIES

All Users must: -

Comply with all relevant parts of this Policy at all times when using the IT Systems.

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.

Immediately inform the Managing Director of any and all security concerns relating to the IT Systems.

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.

Report any and all deliberate or negligent breaches of this Policy by users, which will be handled, as appropriate, under the Company's disciplinary procedures.

7. SOFTWARE SECURITY MEASURE

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.

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.

No Users may install any software of their own, whether that software is supplied on physical media (e.g. DVD-Rom, USB) or whether it is downloaded, without the approval of the Company.

All software will be installed by a qualified and approved supplier.

8. ANTI-VIRUS SECURITY MEASURES

IT Systems (including all computers and routers) will be protected with suitable antivirus, 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.

All systems protected by anti-virus software are subject to constant monitoring.

The Company does not permit the use of storage media (e.g. USB memory sticks or disks of any kind) on its systems.

All files being sent to third parties outside of the Company by email is scanned for malicious software via Microsoft Exchange in-built security measures.

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.

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.

9. HARDWARE SECURITY MEASURES

Wherever practical, desktops 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.

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 Company's Director. Under normal circumstances whenever a problem with such IT System 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.

All hardware containing personal or confidential information must be subject to hardware hardening to include data encryption as a minimum.

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.

The Company shall maintain a complete asset register of all IT Systems.

10. ACCESS SECURITY

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. Such alternative forms of secure log-in may include fingerprint identification, one-time auto generated passcodes and facial recognition.

All passwords must, where the software, computer or device allows and where a perceived risk is present:

- be a minimum of 12 characters long;
- contain a combination of upper and lower-case letters, numbers and symbols;
- be changed annually;
- not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events or places etc.);

- not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events or places etc.);
- be created by individual users and;
- where possible systems to be locked down to company IP address and/or multifactor authentication is to be implemented.

Passwords should be kept secret by each user. Under no circumstances should a user share their password with anyone. 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.

The usage of a password vault is recommended and Legate will provide access to Nordpass for employees to use. The passwords stored within the vault must not be written down and they must be changed when either prompted via the service or annually.

If a user forgets their password, this should be reported to the Company's IT support. They 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.

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).

Users may not use any software that allows outside parties (except for the Company's authorised IT support) to access the IT Systems without the express consent of the Company's 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 Company's Director and the Company's IT support.

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 Company's Director. Any and all instructions and requirements provided by the Company 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 Company's Director shall reserve the right to request the immediate disconnection of any such devices without notice.

11. 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: -

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

12. DATA PROTECTION

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.

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.

13. INTERNET AND EMAIL USE

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. 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.

14. REPORTING IT SECURITY BREACHES

All concerns, questions, suspected breaches or known breaches shall be referred immediately to the Company's Director in accordance with the Company's Incident and Cyber Security Management Policies.

Upon receiving a question or notification of a breach, the Company's Director 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.

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

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

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