1. Introduction

This document sets out the measures to be taken by all employees of NetCollaborators Ltd (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

1. All IT Systems are to be protected against unauthorised access.
2. All IT Systems are to be used only in compliance with relevant Company Policies.
3. All data stored on IT Systems are to be managed securely in compliance with all relevant parts of the Data Protection Act 1998 and all other laws governing data protection whether now or in the future in force.
4. All employees of the Company and any and all 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.
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.
6. All IT Systems are to be installed, maintained, serviced, repaired and upgraded by the Company or by such third party/parties as the Company may from time to time authorise.
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 unless expressly stated otherwise.
8. All breaches of security pertaining to the IT Systems or any data stored thereon shall be reported and subsequently investigated by the Company.
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.

3. The Company's Responsibilities

1. The Company shall:
   a) ensure that all IT Systems are assessed and deemed suitable for compliance with the Company's security requirements;
   b) ensure that IT security standards within the Company are effectively implemented and regularly reviewed; and
   c) keep abreast 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.
2. The Company will:
   a) assist all Users in understanding and complying with this Policy;
   b) provide all Users with appropriate support and training in IT security matters and use of IT Systems;

NetCollaborators Ltd a limited company registered in England and Wales. **Registered Number:** 05202931
Registered Office: 16 Whitehill Close, Camberley, SURREY, GU15 4JR . Tel: 01276 512975 . **website:** www.netcollaborators.com

c) ensure 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) receive and handle all reports relating to IT security matters and take appropriate action in response;

e) take proactive action, where possible, to establish and implement IT security procedures and raise User awareness;

f) monitor all IT security within the Company and taking all necessary action to implement this Policy and any changes made to this Policy in the future; and

g) ensure that regular backups are taken of all data stored within the IT Systems at intervals no less than one day and that such backups are stored at a suitable location off the Company premises.

4. Users' Responsibilities

1. All Users must comply with all relevant parts of this Policy at all times when using the IT Systems.
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.
3. Users must immediately inform the Company of any and all security concerns relating to the IT Systems.
4. Users must immediately inform the Company of any other technical problems (including, but not limited to, hardware failures and software errors) which may occur on the IT Systems.
5. Any and all deliberate or negligent breaches of this Policy by Users will be handled as appropriate under the Company's disciplinary or legal procedures.

5. Software Security Measures

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 Company. This provision does not extend to upgrading software to new 'major releases' (e.g. from version 1.0 to version 2.0), only to updates within a particular major release (e.g. from version 1.0 to version 1.0.1 etc.). Unless a software update is available free of charge it will be classed as a major release and thus falls within the remit of new software procurement and outside the scope of this provision.
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.
3. No User 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. Any software belonging to Users must be approved by the Company and may only be installed where that installation poses no security risk to the IT Systems and where the installation would not breach any licence agreements to which that software may be subject.
4. All software will be installed onto the IT Systems by the Company unless an individual User is given written permission to do so by the Company. 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

1. IT Systems (including all computers and servers) 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.
2. All IT Systems protected by anti-virus software will be subject to a full system scan once a day for the hosted VPS server and weekly for local devices.
3. All storage media (e.g. USB memory sticks or disks of any kind) used by the Company for transferring files must be encrypted and virus-scanned before any files may be transferred. Such virus scans shall be performed upon connection / insertion of media**.**
4. The Company shall be permitted to transfer files using cloud storage systems. All files downloaded from any cloud storage system must be scanned for viruses during the download process.
5. Any files being sent to third parties outside the Company, whether by email, on physical media or by other means (e.g. File Transfer protocols or shared cloud storage) must be scanned for viruses before being sent or as part of the sending process, as appropriate. All email attachments are scanned automatically upon sending.
6. Where any virus is detected by a User this must be reported immediately to the Company (even where anti-virus software has automatically fixed the problem). The Company shall promptly take any and all necessary action to remedy the problem. Where any User deliberately introduces any malicious software or virus to the Company's IT Systems this will constitute a criminal offence under the Computer Misuse Act 1990 and will be handled appropriately.

7. Hardware Security Measures

All User data, websites, emails and files supporting those services and systems are held on our own Linux Virtual Private Server managed and hosted by a UK-based fully professional GDPR-compliant hosting company,

Services include:-

1. UK-based data centres with "Tier 4" availability/uptime (the highest level) on a network backed by BGP redundancy (a method for ensuring network availability continues in the case of a network device or path failure and unavailability).
2. 24 hour a day, 7 days a week, 365 days a year support
3. Full domain backups (including websites, hosted emails) held on separate site using the R1soft backup manager for 2 days and then on a 2 weekly, 3 monthly restorable basis.
4. Security services (including but not restricted to) cPHulk Brute Force Protection, disabled Compiler Access, availability of Security Polices for cPanel webmail on request, Security logging, Security advisor application to check for out-of-date or missing security and automatedly alerting the Company, PHP open_basedir protection preventing Users from opening files outside of their home directory with php, and SMTP Restriction in place to prevent Users from bypassing the mail server to send mail, a common practice used by spammers.

5. Emails and websites are encrypted (evidenced by SSL and https connections). File transfer between encrypted local machines and the data centre is carried out using SSL via the Secure File Transfer Protocol (SFTP)

Company hardware precautions

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 Company premises. If any such mobile device is to be left in a vehicle it must be stored out of sight.

8. **Access Security (How the Company accesses the Data Centre systems)**

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. Such alternative forms of secure log-in may include fingerprint identification and facial recognition.
2. All passwords must, where the software, computer or device allows:
    1. be at least 15 characters long;
    2. contain a combination of upper and lower case letters / numbers / spaces / symbols etc.;
    3. be unique
    4. be different from the previous password;
    5. not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events or places etc.); and
    6. be created by individual Users.
    7. not be written down unless such document is securely kept under lock and key at all times

    The use of a password manager to facilitate this process is therefore strongly recommended.
3. Passwords should be kept secret by each User. Under no circumstances should a User share their password with anyone including within the Company. 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.
4. If a User forgets their password, this should be reported to the Company. The Company 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 the member Staff responsible for resolving the issue. A new password must be set up by the User immediately upon the restoration of access to the IT Systems.
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 10 minutes of inactivity. Activation of the

screensaver will not interrupt or disrupt any other activities taking place on the computer (e.g. data processing).

6. Users may not use any software which may allow outside parties to access the IT Systems without the express consent of the Company. 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.

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 Company. 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 shall reserve the right to request the immediate disconnection of any such devices without notice.

9. Data Protection

1. All personal data (as defined in the Data Protection Act 1998) 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 1998, the provisions of the Data Protection Act 1998 and the Company's Data Protection Policy.

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.

10. Internet and Email Use

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.

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.

11. Reporting IT Security Breaches

1. All concerns, questions, suspected breaches or known breaches shall be referred immediately to the Company.

2. Upon receiving a question or notification of a breach, the Company shall, within one day assess the issue including, but not limited to, the level of risk associated therewith, and shall take any and all such steps as the Company deems necessary to respond to the issue.

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

4. All IT security breaches, whether remedied by the Company or by a User under the Company's direction, shall be fully documented.

12. **Implementation of Policy**

This Policy shall be deemed effective as of 9 March 2018. 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:	James Geoffrey Strong
Position:	Director
Date:	9 March 2018
Signature:	

End of Document

NetCollaborators Ltd a limited company registered in England and Wales. **Registered Number:** 05202931
Registered Office: 16 Whitehill Close, Camberley, SURREY, GU15 4JR . Tel: 01276 512975 . **website:** www.netcollaborators.com