IT COMMUNICATION & MONITORING POLICY

Introduction:

SB Security Solutions Limited provides you with access to various computing, telephone and postage facilities ("the Facilities") to allow you to undertake the responsibilities of your position and to improve internal and external communication.

Policy Information:

This Policy sets out the Company's policy on your use of the Facilities and includes:

- Your responsibilities and potential liability when using the Facilities.
- The monitoring policies adopted by the Company.
- Guidance on how to use the Facilities.

This Policy has been created to:

- Ensure compliance with all applicable laws relating to the Data Protection Act, as amended 2018 and the UK GDPR 2021, information security and compliance monitoring.
- Protect the Company and its employees from the risk of financial loss, loss of reputation or libel.
- Ensure that the Facilities are not used so as to cause harm or damage to any person or organisation.

This Policy applies to the use of:

- Local, inter-office, national and international, private or public networks (including the Internet and Intranet) and all systems and services accessed through those networks.
- Desktop, portable and mobile computers and applications (including personal digital assistants, ipads & any derivatives).
- Mobile telephones, iPhone, smart phones or any derivatives (including the use of WAP services).
- Electronic mail and messaging services.

Observation of this Policy is mandatory and forms part of the Terms and Conditions of employment. Misuse of the Facilities will be treated as gross misconduct and may lead to dismissal.

Computer Facilities - Use of Computer Systems:

Subject to anything to the contrary in this Policy, the Facilities must be used for business purposes only.

In order to maintain the confidentiality of information held on or transferred via the Company's Facilities, security measures are in place and must always be followed. A log-on ID and password is required for access to the Company's network. Despite your use of a password, the Company reserves the right to override your password and obtain access to any part of the Facilities.

You are responsible for keeping your password secure. You must not give it to anyone, including colleagues, except as expressly authorised by the Company.

You are expressly prohibited from using the Facilities for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Company or its clients other than in the normal and proper course of carrying out your duties for the Company.

In order to ensure proper use of computers, you must adhere to the following practices:

- Anti-virus software must always be kept running.

- All other forms of media storage must be checked by your Line Manager before the contents are accessed or stored on the Company's network or hard drives.
- Obvious passwords such as birthdays and spouse names etc must be avoided. The most secure passwords are random combinations of letters and numbers.
- When you are sending data or software to an external party by flash drive or USB always ensure that it has been checked for viruses by your Line Manager before sending it.
- All files must be stored on the network drive which is backed up regularly to avoid loss of information.
- Always log off the network before leaving your computer for long periods of time or overnight.

Software:

Software piracy could expose both the Company and the user to allegations of intellectual property infringement. The Company are committed to following the terms of all software licences to which the Company is a contracting party. This means that:

- Software must not be installed onto any of the Company's computers unless this has been approved in advance by your Line Manager. They will be responsible for establishing that the appropriate licence has been obtained, that the software is virus free and compatible with the computer Facilities.
- Software should not be removed from any computer nor should it be copied or loaded on to any computer without the prior consent of your Line Manager.

Laptop Computers:

At various times during your employment with the Company, you may use a laptop. These computers, along with related equipment and software are subject to all the Company's policies and guidelines governing non-portable computers and software (see two paragraphs in software section above). However, use of a laptop creates additional problems especially in respect of potential breaches of confidentiality. When using a laptop:

- You are responsible for all equipment and software until you return it. The laptop must always be kept secure.
- You are the only person authorised to use the equipment and software issued to you.
- You must not load or install files from any sources without your Line Manager inspecting such files for viruses.
- All data kept on the laptop must be backed up regularly in order to protect data against theft or mechanical failure or corruption.
- You must password protect confidential data on USBs or on the hard drive to protect against theft.
- If you discover any mechanical, electronic, or software defects or malfunctions, you should immediately bring such defects or malfunctions to the attention of your Line Manager.
- Using the laptop, or any other IT Media provided by the company, for personal files, documentation, photographs etc is not authorised, nor a reason not to return company property if required. Upon the request of the Company at any time, for any reason, you will immediately return any laptop, equipment and all software to the Company.
- If you are using your own laptop to connect with the Company's network or to transfer data between the laptop and any of the Company's computers you must ensure that you have obtained prior consent from your Line Manager, comply with their instructions and ensure that any data downloaded or uploaded is free from viruses.

email (Internal or External Use):

Internet email is not a secure medium of communication – it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If you are sending confidential information by email this should be sent using password protected attachments.

Email should be treated as any other documentation. If you would normally retain a certain document in hard copy you should retain the email.

Do not forward email messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the email.

Your email inbox should be checked on a regular basis.

As with many other records, email may be subject to discovery in litigation. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.

You are to consult your Assignment Instructions or contact your Line Manager to ascertain whether you may use email for private purposes. If agreed; then you must ensure emails contain the following message:

"This email does not reflect the views or opinions of SB Security Solutions Limited"

If Internet email facilities are permitted; it is done so providing that:

- Such emails do not contain information or data that could be obscene, racist, sexist, otherwise offensive and provided that such use is not part of a pyramid or chain letter.
- Such emails are not used for the purpose of trading or carrying out any business activity other than Company business.

If you are away from the office and use email as an external means of communication, you must ensure the auto reply service is used to inform the sender that you are unavailable. Failure to do so could lead to disciplinary action. If you have any doubt as to how to use these Facilities; contact your Line Manager.

Internet:

Use of the Internet, or Internet services, by unauthorised users is strictly prohibited. You are responsible for ensuring you are the only person using your authorised Internet account and services.

Downloading any files from the Internet using the computer Facilities is not permitted. If there is a file or document on the Internet which you wish to acquire, contact your Line Manager to plan for it to be evaluated and checked for viruses. It will be at the discretion of your Line Manager whether to allow such a download.

Viewing, downloading, storing (including data held in RAM or cache) displaying or disseminating materials (including text and images) that could be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use are strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.

Posting information on the Internet, whether on a newsgroup, via a chat room or via email is no different from publishing information in the newspaper. If a posting is alleged to be defamatory, libellous, or harassing, the employee making the posting and the Company could face legal claims for monetary damages.

Using the Internet for the purpose of trading or carrying out any business activity other than Company business is strictly prohibited.

You are to consult your Assignment Instructions or contact your Line Manager to ascertain whether you may use the Internet for private purposes.

For the avoidance of doubt the matters set out above include use of WAP facilities.

Monitoring Policy:

The Policy of the Company is that we may monitor your use of the Facilities.

The Company recognises the importance of an individual's privacy but needs to balance this against the requirement to protect others and preserve the integrity and functionality of the Facilities.

The Company may from time to time monitor the Facilities. The principal reasons for this are to:

- Detect any harassment or inappropriate behaviour by employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies.
- Ensure compliance of this Policy.
- Detect and enforce the integrity of the Facilities and any sensitive or confidential information belonging to or under the control of the Company.
- Ensure compliance by users of the Facilities with all applicable laws (including Data Protection), regulations and guidelines published and in force from time to time.
- Monitor and protect the well-being of employees.

The Company may adopt at any time a number of methods to monitor use of the Facilities. These may include:

- Recording and logging of internal, inter-office and external telephone calls made or received by employees using its telephone network (including where possible mobile telephones). Such recording may include details of length, date and content.
- Recording and logging the activities by individual users of the Facilities. This may include opening emails and their attachments, monitoring Internet usage including time spent on the Internet and web sites visited.
- Physical inspections of individual user's computers, software and telephone messaging services.
- Periodic monitoring of the Facilities through third party software including real time inspections.
- Physical inspection of an individual's post.
- Archiving of any information obtained from the above including emails, telephone call logs and Internet downloads.

If at any time an employee wishes to use the Facilities for private purposes without the possibility of such use being monitored they should contact their Line Manager. This person will consider such request and any restrictions upon which such consent is to be given. In the event such a request is granted, the Company (unless required by law) will not monitor the applicable private use.

The Company will not (unless required by law):

- Allow third parties to monitor the Facilities.
- Disclose information obtained by such monitoring of the Facilities to third parties.

The Company may be prohibited by law from notifying employees using the Facilities of a disclosure to third parties.

Display Screen Equipment (DSE) – Annual Questionnaire:

Staff at Head Office with workstations and any receptionist staff (with DSE), which is being used as an

integral part of their employment are to complete an annual HSE approved DSE questionnaire. Staff who are new in post are to complete an initial questionnaire, which will be collated through our HR department. Any actions required, as a result of these questionnaires, are to be arranged through the Office Manager or client site representative.

General Guidance:

Never leave any equipment or data (including client files, laptops, computer equipment, mobile phones and PDAs) unattended on public transport or in an unattended vehicle.

When using email or sending any form of written correspondence:

- Be careful what you write. Never forget that email and written correspondence are not the same as conversation. They are a written record and can be duplicated.
- Use normal capitalisation and punctuation. Typing a message all in capital letters is the equivalent of shouting at the reader.
- Check your grammar and spelling.
- Do not forget that emails and other forms of correspondence should maintain the high standards expected by the Company. Where applicable you should use formal headings and introductions such as “Dear...” and,” Yours sincerely”.
- There are new UK GDPR regulations (implemented in January 2021). You must read and comply with the requirements of SBS Policy documentation: **QD.14 GDPR Statement & Privacy Policy.**

Observation of this Policy is mandatory and forms part of the Terms and Conditions of Employment. Misuse of the Facilities will be treated as gross misconduct and may lead to dismissal.

Implementation:

The implementation of this policy is the responsibility of the Managing Director; assisted by the Data Controller, Senior Operations Manager and nominated Line Management.

Review:

This policy shall be reviewed and updated annually & if legislation, regulation, or policies change.

S Bettesworth

Steve Bettesworth
Managing Director