INFORMATION SECURITY POLICY

1.0 Purpose

The purpose of this policy is to establish standards for the protection and security of all information held and processed by Virtual Business Source Ltd (VBS). Effective implementation of this policy will minimize the risk of loss or unauthorised access to VBS and client information and technology.

This policy provides an overview of the systems and procedures that VBS use to protect information.

2.0 Scope

This policy applies to all VBS staff and systems.

In respect of Personal Data VBS will comply with the Data Protection Act 1998 and after 25 May 2018 with the General Data Protection Regulation ((EU) 2016/679). Together both are referred to here as the Data Protection Legislation.

3.0 Policy

3.1 Ethics and Acceptable Use Policies

VBS expects that all employees conduct themselves in a professional and ethical manner. An employee should not conduct business that is unethical or illegal in any way, nor should an employee influence other employees to act unethically or illegally. Furthermore, an employee should report any dishonest activities or damaging conduct to an appropriate line manager.

Security of client information is extremely important to our business. We are trusted by our clients to protect sensitive information that may be supplied while conducting business. Sensitive information is defined as any personal information (i.e. - name, address, phone number, e-mail, Social Security number, bank account, credit card numbers, tax or income details, etc.) or company information not publicly available (i.e. – clients' financial information, employee information, accounts, technology, etc.). It is important that employees do not reveal sensitive information about VBS or our clients to outside resources that do not have a need to know such information.

3.2 Personal Data

VBS shall only process Personal Data (a) for the purposes of providing services to clients or (b) as otherwise expressly authorised by the data subject.

VBS shall maintain any valid and up-to-date registration or notification required under the Data Protection Legislation.

VBS shall implement appropriate technical and organisational measures to protect Personal data against unlawful processing and against accidental loss, destruction, damage, alteration or disclosure of the Personal data including encrypting all Personal Data stored and/or processed on all digital or electronic portable storage devices.

VBS shall not process personal data outside the European Economic Area without prior written consent.

VBS will promptly notify clients if (a) the subject of any Personal Data related to them makes a written request to have access to Personal Data or any complaint or request relating to the clients obligations under the Data Protection Legislation, or (b) it becomes aware of any loss, damage, destruction, or unauthorised processing or accidental disclosure of Personal Data in accordance with the Data Breach & Incident Management Plan.

3.3 Protect Stored Data

VBS will protect sensitive information stored or handled by the company and its employees. All sensitive information must be stored securely and disposed of in a secure manner when no longer needed for business reasons.

Access to the VBS computer systems requires a username and password. Each user has a unique username and is given access to applications and data based on their business function. User accounts are managed by the VBS IT department on instruction from the HR department and Directors. Staff leaving VBS will have their access rights and permissions revoked at the earliest opportunity.

Any media (i.e. - paper, USB memory stick, disk, backup tape, computer hard drive, etc.) that contains sensitive information must be protected against unauthorised access. This will include physical protection and, where possible, technological protection such as disk or file encryption.

Media no longer needed must be destroyed in such a manner to render sensitive data irrecoverable. This will include shredding of paper, physical destruction of tapes, compact disks, DVDs, and floppy disks, and secure wiping of hard disks.

VBS will carry out routine backups of all client data held on the computer network. These backups will be tested regularly to ensure data can be recovered in case of loss on the live systems.

3.4 Protect Data in Transit

If sensitive information needs to be transported physically or electronically, it must be protected while in transit (i.e. - to a secure storage facility or across the Internet).

All VBS portable computers (laptops) will be password protected. VBS also issues encrypted portable USB devices for the secure transfer of data. Transmission of sensitive data via the Internet shall only be via secure SSL transmission to recognized locations (such as transmission of tax information to HMRC) or by encrypted emails.

3.5 Restrict Access to Data

In order to provide a high level of service VBS will regularly share information about clients within the organization. However, VBS will restrict access to particularly sensitive information (business data and personal information such as payroll details) to those that have a need-to-know.

3.6 Physical Security

VBS will restrict physical access to sensitive information and systems that house that information (i.e. computers or filing cabinets storing data), to protect it from those who do not have a need to access that information.

• All servers holding data will be held in a secure locked room with access limited to authorized individuals.

• VBS take appropriate security measures to protect their offices outside office hours, including alarm systems, door locks, and CCTV.

• Access to all VBS offices is protected by keycode locks.

• Visitors should always be escorted and easily identifiable when in areas that may contain sensitive information.

• Password protected screen savers will be used on all computers.

3.7 Security Awareness and Procedures

Keeping sensitive information secure requires periodic training of employees and contractors to keep security awareness levels high. The following policies and procedures address this issue:

• VBS will hold periodic security awareness training meetings of employees and contractors to review correct handling procedures for sensitive information.

• Employees are required to comply with the VBS acceptable use policies which form part of the VBS Employee handbook.

• Background checks (such as criminal record checks, within the limits of local law) may be conducted where appropriate for employees that handle sensitive information.

• VBS security policies will be reviewed annually and updated as needed.

3.8 Data Breach & Incident Management Plan

There will be an employee of the company designated as the information security officer. The security officer is responsible for communicating security policies to employees and

contractors and tracking the adherence to policies. In the event of a compromise of sensitive information, the security officer will oversee the execution of the Data Breach & Incident Management Plan.

4.0 Enforcement

Failure by an employee to comply with the standards and policies set forth in this document may result in disciplinary action up to and including termination of employment.

Version 9 March 2018