INFORMATION SECURITY POLICY

1. Introduction

The Company must protect its information assets – defined for the purposes of this Policy as computers, hardware, networks, software and all of the data they contain - and its reputation. This will help the Company to:

- Ensure that a high quality service is offered to our staff and customers.
- Ensure that it does not lose opportunities for funding through a poor reputation for information security.
- Maintain and improve its reputation and meet its legal obligations and strategic business and professional goals.
- Prevent data loss, including research and teaching data, and criminality.
- Ensure that staff are fully aware of their personal responsibilities for protecting data in accordance with Company or any external organisation's guidelines.

2. Objective

This Policy addresses the security of the Company's information assets as defined above.

The Policy's objective is to protect SludgeTEK Ltd from information security incidents that might have an adverse impact on its operations, reputation and professional standing.

Information security incidents include but are not limited to: confidentiality (the wrong people obtaining information); integrity (information being altered without permission, whether deliberate or accidental) and availability (information not being available when it is required).

The widest possible definition of information security will be used to include all types of incident that impact the effective use of information. This includes the performance, robustness, reliability and accuracy of equipment, electronic or paper systems and data.

The scope of this policy is all of the Company's information. This initial version of the document sets out a framework and addresses the organisation's corporate data, touching in addition on research and teaching related data. Subsequent refinements, based on wider consultation, will reflect as many individual needs as possible.

3. Principles

3.1 Approach

- Use all reasonable, appropriate, practical and effective information security measures, including internationally recognised standards and the classification of information, to protect important processes and assets. This will also include practical measures such as encrypting memory sticks and managing passwords.
- Recognise the concepts of appropriate company and staff freedom, and the value of collaboration. Such freedom also brings responsibilities. The needs of the individual as well as the organisation will always be considered in the context of this Information Security Policy as well as legal and contractual requirements.
- Continually examine ways in which information security measures can be improved, in order to protect and enhance the Company's operations.

- The Company will protect and manage its information assets to enable it to meet its contractual, legislative, privacy and ethical responsibilities.

3.2 Responsibilities

- The General Manager is responsible for overseeing the security of the Company's Information Assets.
- Everyone granted access to SludgeTEK Ltd's computing and information systems is responsible for protecting its information assets and likewise protecting the information assets of those third parties to which access is granted.
- All members of the Company are responsible for reporting shortfalls in existing information security practices and suggesting improvements that could be made to the General Manager

3.3 Sensitivity of information

- Much of the information in the Company is not confidential. In many cases, it is desirable to share information as widely as possible. This policy applies to the safe keeping of both confidential and non-confidential information. Specific measures will apply to confidential information.
- The Company's definition of what constitutes confidential and non-confidential information is in the Company's GDPR & Privacy policy.
- Information will be shared as appropriate within and outside the Company in order to facilitate business. Information may be designated as, or otherwise considered to be, confidential. However, the Company has obligations under the Data Protection Act 2018 and, under the Freedom of Information Act 2000 which mean that information designated as 'confidential' may have to be disclosed. The DPO is available to advise on whether a record must be disclosed.

3.4 Practices

- Risk analysis techniques will be used to identify information security risks and their relative priorities. Identified risks will be responded to promptly, implementing safeguards that are appropriate, effective, culturally acceptable and practical.
- Wherever practicable, rights to access and process information will be granted to roles and then people matched to those roles.
- Wherever practicable, all actions will be attributable to an identified individual.
- All use of computer and information systems and information (including third party information) will be attributable, protected by safeguards and handling rules in accordance with current legislation.
- The Company will routinely monitor information systems usage, in line with current legislation, to assure the continued integrity and security of the Company's information systems and to assist in the resolution of an information security incident.
- The Company will ensure that its activities can continue with minimal disruption, or other adverse impact, should it suffer any information security incident. This will be done in line with the Company's Business Continuity Plan.
- Actual or suspected information security incidents will be reported promptly to the GENERAL MANAGER or via the Company's Procedure. The General Manager will allocate the incident to an appropriate member of the management team who will manage the Incident to closure and analyse it for lessons to be learnt. In every material case the Managing Director will be informed.

- The General Manager will have delegated responsibility for maintaining detailed Information Security Procedures which will cover each of the areas of this policy.
- Documented Guidelines, education and training will supplement this Information Security Policy.

The General Manager will monitor compliance with, and the effectiveness of the Policy on a regular basis, on behalf of SludgeTEK Ltd. The General Manager will review, and bring forward for approval, revisions to the Information Security Policy as appropriate.

4. Policy Awareness

The General Manager will publicise this Information Security Policy to all members of the Company and others granted access to Company computing facilities. All such members and guests of the Company are expected to be familiar, and to comply, with the Information Security Policy and Guidelines. The General Manager or nominee will be responsible for interpretation of the Information Security Policy.

5. Applicability and Enforcement

This Policy and compliance with it applies to all members of SludgeTEK Ltd and its sub companies and to others who use its computer and information systems.

The General Manager is responsible for ensuring that suitable guidelines, education and training are in place to assist all members of SludgeTEK Ltd in complying with this policy.

The General Manager or nominee will be responsible for ensuring that any transgression of this policy is dealt with using the Company's disciplinary procedures as appropriate.

SludgeTEK Ltd will require all joint ventures to adopt Information Security Policies which are broadly consistent with this document and will not allow access to the Company's Information Assets until it is satisfied that appropriate arrangements are in place.

Date: 2nd August 2021