

# GREYSTONE MANAGED SERVICES LIMITED

## ACCEPTABLE USE POLICY

### 1 General

- 1.1 Greystone Managed Services Limited ("**Greystone**") provides businesses with certain information technology related software products and services, including but not limited to the "Rekoop" product and associated hosting services (together the "**Services**").
- 1.2 This document sets out Greystone's "Acceptable Use Policy" with a view to ensuring the integrity, security, reliability and privacy of Greystone's network, systems, products, services, hosting facilities and data contained therein (collectively the "**Network**").

### 2 Client Network Configuration

- 3.1 The Services are delivered over the Internet. You shall provide all users with secure Internet access at your own cost. Greystone is only responsible for the provision of the Services up to and including the public internet gateway located within Greystone's data centre facility.
- 3.2 The Services must be assigned a valid IP address within your own network. Any resultant change to the internal address of your systems shall be your responsibility and shall be carried out at your own cost.

### 3 Acceptable Use

- 3.1 You shall not (and shall procure that the users of the Services shall not):
  - 3.1.1 allow any unauthorised user or third party access to, or use of the Services and shall take all reasonable security measures to prevent the same;
  - 3.1.2 add to, modify or interfere in any way with the Services;
  - 3.1.3 use the Services in any way that:
    - (a) violates any applicable law, regulation, administrative order or treaty;
    - (b) would constitute or contribute to the commission of a crime, tort, fraud or other unlawful activity (including activities deemed unlawful under a complainant's jurisdiction) or to transmit any material which may be abusive or menacing;
    - (c) involves violations of systems or networks (hacking) or to attempt to violate security by any method for example port scanning and packet sniffing; or
    - (d) interferes with (or is intended to interfere with) systems or networks ability to operate (denial of service);
  - 3.1.4 deliberately use forged (spoofed) or corrupted IP packets;
  - 3.1.5 use network broadcast packets (smurfing); or
  - 3.1.6 use the Services for the purposes of sending, posting, publishing, distributing, disseminating or transmitting any message communication or material which:
    - (a) is offensive, abusive, indecent, obscene, harassing or menacing illegal, threatening, defamatory, discriminatory or promotes illegal or unlawful activity;
    - (b) is unsolicited, chain mail, of a junk-mail or a spam-like nature, relates to or promotes pyramid schemes or contains falsified or missing header information;
    - (c) is fraudulent or defamatory or contains, without the appropriate permission, another person's proprietary information (including intellectual property);
    - (d) is discriminatory or contrary to any UK race, disability or sex discrimination legislation; or

- (e) is sent, posted, published, distributed, disseminated or transmitted in an illegal or malicious manner, for an illegal or malicious purpose or without due regard to and, without the use of reasonable care to avoid, the transmission or dissemination of spam, viruses or other malicious mailings or code.

- 3.2 You shall ensure that your staff and any other users of the Services shall comply with and shall keep any passwords and/or information about security policies and procedures provided to it by Greystone in relation to the provision of the Services secure and shall promptly inform Greystone of any unauthorised disclosure of such passwords or information or of any other circumstance which may require that any passwords notified be changed.

#### **4 Protection against Viruses**

- 4.1 Greystone shall use its reasonable endeavours to keep the Services virus-free to the extent that it is provided via networks within Greystone's direct control.
- 4.2 You shall keep the Service secure and free of viruses, adware, malware, spyware, worms and other hostile codes by installing and updating adequate anti-virus and security software on each of your mobile devices and or systems which use the Software from time to time.

#### **5 Liability**

- 5.1 The Internet is a unique coming together of different networks spanning all the world's countries. As such Greystone is unable to control the content of material coming into or passing through its Network.
- 5.2 Greystone is not liable for any material found to have passed through its chosen carrier's network or servers or to have originated on any part of their chosen carrier's telecommunications network. Where any such material is brought to the attention of Greystone, Greystone will investigate and may take action as appropriate but cannot guarantee any action will be taken, especially where third parties are involved.
- 5.3 If you have any concerns regarding information that has passed across a carrier's telecommunications network we recommend that you contact directly the administrator responsible for the area of the Internet with which a complaint originates.
- 5.4 Greystone is connected to the global Internet through many transit and peering connections. Whilst Greystone adheres to any service level laid out in a service contract it cannot guarantee optimum connectivity (or for more serious occurrences any connectivity) to all areas of the Internet.

#### **6 Reporting**

- 6.1 If Greystone becomes aware that the Services are being used contrary to this Acceptable Use Policy, Greystone shall promptly notify you of any such non-compliance and you shall cease such activities and shall ensure that sufficient steps are taken to prevent the repetition of such non-compliance.
- 6.2 If you suspect or become aware that a user of the Services is in breach of this policy, please send details of the incident to [support@greystone-services.com](mailto:support@greystone-services.com). To enable Greystone to investigate the matter promptly and efficiently please provide as much information as possible, including the exact date, time and time zone, where applicable IP address and any other relevant information relating to the incident.
- 6.3 Greystone takes each complaint seriously. Please allow up to two (2) working days for an initial response or acknowledgement to be provided. Greystone cannot guarantee that action will be taken from the information provided.
- 6.4 If you are dissatisfied with how a complaint has been resolved, Greystone shall be happy to discuss this to a reasonable conclusion.