BEDROQ ACCEPTABLE USE POLICY

This Acceptable Use Policy (AUP) ("Service Schedule") forms part of to the Managed Services Agreement (the "Agreement") as entered into between the Parties. All terms defined herein shall have the same meaning as the terms defined in the Agreement unless specifically set out herein. The terms of the Agreement shall be incorporated into this Service Schedule and this Service Schedule shall form part of the Agreement. To the extent of any conflicts arising between the terms of the Agreement and the terms of this Service Schedule, the terms of this Service Schedule shall prevail.

It has been formulated with the following goals in mind:

- to give the Client a better understanding of what is and what is not acceptable when using the Supplier's Managed Services.
- to ensure security, reliability and integrity of the Supplier's systems and network, systems as well as the networks and systems of the Client, and the networks and system of others.
- to avoid situations that may cause the Supplier to incur civil liability and to comply with legal requirements concerning the use and/or misuse of a public communication system as defined by legislation such as the Telecommunications Act.
- to preserve the privacy and security of individual users.
- to ensure the Client avoids engaging in activities which directly or indirectly may have a detrimental impact on the Supplier or the Client.
- to preserve to good reputation of the Supplier as a high quality, professional service provider.

The AUP below defines the actions which the Supplier considers to be abusive and unacceptable, and thus, strictly prohibited. The items are not exclusive, and the list should not be considered exhaustive.

The Supplier reserves the right to amend, modify or substitute this AUP from time to time. The continued use of the Managed Services provided by the Supplier signifies that the Client agrees to be bound by this AUP and by any amendments to it.

1 GENERAL

1.1 The Managed Services may only be used for lawful purposes. Transmission, distribution, or storage of any information, data or material in violation of Applicable Laws is prohibited. This includes, but is not limited to, material protected by copyright, trademark, trade secret or infringement of other Intellectual Property Rights of others or the privacy, publicity or personal rights of others. The Supplier reserves the right to remove such illegal material from its servers.

1.2 Client's are prohibited from transmitting on or through any of the Managed Services, any material that is, in Suppliers' sole discretion, unlawful, obscene, threatening, abusive, libellous, hateful, or encourages conduct that would constitute a criminal offence, give rise to civil liability, or otherwise violate any Applicable Law.

1.3 The resale of Supplier products and the Managed Services is not permitted, unless specifically authorised in a written agreement.

1.4 Supplier reserves the right to restrict access to the Managed Services where it is deemed the Client is using it in a way which exceeds the Suppliers' double the average number of support requests, when measured over a three month period against Client's with similar agreements. In all cases relating to this matter, Supplier will first engage with the Client to discuss appropriate changes, or contracting of new Services to match those required by the Client.

1.5 Client accounts on Supplier systems must have a password which is at least 8 mixed alpha, numeric and special characters with case variations. The Client should not permit a common word to be used as a password. You must protect the confidentiality of your password, and you should change your password regularly. If you have forgotten a password used for your Supplier, then contact our support team. From time to time the supplier may revise this policy or require customers to authenticate using other means, including, but not limited to two factor authentication.

1.6 Clients are responsible for violations of this AUP by anyone using the Managed Services with the Client's permission or on an unauthorised basis as a result of the Client's failure to use reasonable security precautions.

1.7 Clients and any third party acting on their behalf must not attempt to probe, scan, penetrate or test the vulnerability of other Supplier customers nor Supplier shared infrastructure or core systems, whether by passive or intrusive techniques.

1.8 Supplier provides Managed Services to the Client, and Clients have no rights to physically access the equipment that supports that service.

1.9 Supplier uses several accounting methods, tools and Services in order to calculate Client consumption charges, any attempt to subvert, obfuscate or otherwise avoid full and accurate charging methods is strictly prohibited.

1.10 Clients are responsible for keeping their billing data with Supplier up-to-date and accurate. Furnishing false data upon signup, contract, or online application, including fraudulent use of credit card numbers, is grounds for immediate termination, and may subject the offender to civil or criminal liability.

1.11 Clients are responsible for keeping their service contact data with Supplier up-to-date and accurate. Any reduction in Service, security threat or security breach brought about directly or indirectly from incorrect or old contact information is the responsibility of the Client.

2 RESPONSIBLE USERS

2.1 The Client, or its authorised agents and third parties using Managed Services supplied under the Agreement must conform to any and all requirements laid out by the following UK Acts/policies:

(a) Computer Misuse Act (1990);

(b) Data Protection Legislation;

(c) Chest Code of conduct;

(d) Regulation of Investigatory Powers Act (2000);

(e) The Counter-Terrorism and Security Act 2015

2.2 The Client, or its authorised agents and third parties using Managed Services supplied under this Agreement may not directly or indirectly download, creation, manipulation, transmit or store:

(a) any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;

(b) unlawful material, or material that is defamatory, threatening, discriminatory, extremist, terrorist or which has the potential to radicalise themselves or others;

(c) unsolicited “nuisance” emails;

(d) material which is subsequently used to facilitate harassment, bullying and/or victimisation of a an individual or a third party;

(e) material which promotes discrimination on the basis of race, gender, religion or belief, disability, age or sexual orientation;

(f) material with the intent to defraud or which is likely to deceive a third party;

(g) material which advocates or promotes any unlawful act;

(h) material that infringes the intellectual property rights or privacy rights of a third party, or that is in breach of a legal duty owed to another party; or

(i) material that brings the Supplier into disrepute.

3 MESSAGING SYSTEMS

3.1 Harassment, whether through language, frequency, or size of messages, is prohibited.

3.2 The Client is explicitly prohibited from sending unsolicited bulk mail messages ("junk mail" or "spam"). This includes, but is not limited to, bulk-mailing of commercial advertising, informational announcements, and political tracts. Such material may only be sent to those who have explicitly requested it. Users of mailing lists must monitor non-deliveries and cleanse their lists accordingly.

3.3 Malicious email of any type is prohibited.

3.4 Forging of header information in any deceitful manner or obscuring the source of an email is not permitted.

3.5 Supplier accounts or Managed Services may not be used to collect replies to messages sent from another Internet Service Provider, where those messages violate this AUP or the Acceptable Use Policy of that other provider.

4 SYSTEMS AND APPLICATIONS

4.1 Clients may not attempt to circumvent user authentication or security of any host, or related user accounts. This includes, but is not limited to, accessing data not intended for the Client,

logging into a server or account the Client is not expressly authorised to access, probing the security of systems or running scanning tools.

4.2 Clients may not attempt to interfere with service to any user or host. This includes but is not limited to deliberate attempts to overload a Service and attempts to make a host unresponsive.

4.3 Users who violate system or application security may incur criminal or civil liability. Supplier will cooperate fully with investigations of violations of systems or network security at other sites, including cooperating with law enforcement authorities and, or UK Security Services in the investigation of suspected criminal violations.

4.4 Supplier reserves the right to run security scanning agents and test mail and web infrastructure connected to the Supplier network for the sole purpose of ensuring system integrity.

4.5 The Client must not attempt to probe, scan, penetrate or test the vulnerability of Supplier Managed Applications and systems, or to breach or attempt to breach the Supplier security or authentication measures, whether by passive or intrusive techniques without prior written agreement from the Supplier Group.

4.6 The Client is prohibited from excessive consumption of shared infrastructure resources, including CPU time, memory, disk space, and session time. The use of resource-intensive programs which negatively impact other system users or the performance of Supplier systems or networks is prohibited, and Supplier staff may, acting reasonably, take action to limit or terminate such programs after communicating its intention to do so.

4.7 The Client must use best efforts to secure any device or network within the Client's control against being used in breach of the Applicable Laws against spam and unsolicited mail, including where appropriate by the installation of anti-virus software, firewall software, and operating and application software patches and updates.

5 NETWORK SECURITY

5.1 The Client may not attempt to circumvent user authentication or security of network. This includes, but is not limited to, accessing data not intended for the Client, probing the security of other networks or running scanning tools.

5.2 The Client may not attempt to interfere with service to any network. This includes but is not limited to deliberate attempts to overload a network or network component.

5.3 The Client must not intentionally use the Supplier network to transmit, distribute or store material that contains a virus, worm, Trojan horse or other harmful component.

5.4 Users who violate network security may incur criminal or civil liability. Supplier will cooperate fully with investigations of violations of systems or network security at other sites, including cooperating with law enforcement authorities and, or UK Government Security Services in the investigation of suspected criminal violations.

5.5 The Supplier reserves the right to run security scanning agents and tools connected to the Supplier network for the sole purpose of ensuring network integrity or troubleshooting issues.

5.6 The Client must use best efforts to secure any device or network within the Client's control against being used in breach of the Applicable Laws or by unauthorised users or third parties.

6 WEB SERVICES

6.1 Any and all data and material held on any managed servers supported or provided by Supplier and network facilities remains the responsibility of the Client.

6.2 Supplier reserves the right to remove or suspend web sites or content delivery servers (such as but not limited to FTP or BITTORRENT) servers at our premises which contain material offensive or are deemed unacceptable by Supplier and such other organisations including ISOC, NHTCU, SOCA or Scotland Yard.

7 AUP BREACH INVESTIGATIONS

7.1 Supplier reserves the right to investigate suspected violations of the AUP. When we become aware of possible violations, we may initiate an investigation, which may include gathering information from the user involved and the complaining party, if any, and examination of material on our servers. Much of the AUP reflects acts that may constitute breaches of Applicable Law and may in some cases carry criminal liability. It is our policy to assist police and law enforcement bodies or UK Security Services in any practicable way when required by Applicable Law.

7.2 During an investigation, we may suspend the account involved and/or remove the material involved from our servers. Such action may include temporary or permanent removal of material from our servers, the cancellation of newsgroup postings, warnings to the user responsible, and the suspension or termination of the account responsible. We will determine what action will be taken in response to a violation on a case-by-case basis.

7.3 The Client acknowledges that the Supplier may be required by current or future law or regulation to access, monitor, store, take copies of, or otherwise deal with the Client's data stored on or transmitted by the Service. Without limitation, you, the Client, expressly authorise us to use your personal data and other account information in connection with any such investigation, including by disclosing it to any third party authority that we consider has a legitimate interest in any such investigation or its outcome.

7.4 Supplier reserves the right to suspend or terminate the Managed Service with immediate effect and without further obligation or liability to the Client as required by any law enforcement organisation in the event the Client breaches any of the terms of this Service Schedule.

8 ACCEPTABLE CHANGE VOLUMES

8.1 The Supplier will undertake for the Client simple, essential changes as part of the Managed Services. If, however, in the sole opinion of the Supplier the changes are vexatious, or of an unreasonably high volume or priority, it reserves the right to charge for those changes on its standard time and material basis.

8.2 Maximum levels of simple change are considered as;

(a) 2 changes to Hypervisor or O/S per server per month.

(b) 2 changes to network component per network component per month.

(c) 5 changes to Managed SAAS App for each Managed SAAS App per month.

(d) 5 changes to each Managed App per Managed App per month,

(e) 2 changes or password resets or account unlocks per user/End User Device per month,

(f) 5 changes to Server Backup or Storage per server per month.

(g) 5 changes to any other part of the Managed Service

Disclaimer

The Supplier does not have any contractual responsibility to monitor any Client activity and we hereby disclaim any responsibility for any misuse of our network.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.