Acceptable Use and Anti-Abuse Policy

The Registry has developed and adopted this Acceptable Use and Anti-Abuse Policy (the "Policy") which is to be read together with other Registry Policies, the Registry-Registrar Agreement, the Registration Agreement, the Registry Agreement and all applicable ICANN policies, as amended from time to time. Unless the context or the Definitions for Policies document published on the Registry Website otherwise require, defined terms used in this Policy shall have the same meanings given to them in the Registry-Registrar Agreement.

Please note that the Registry may modify this Policy from time to time effective upon sixty (60) calendar days' notice to interested parties, including each Registrar, who shall inform its Registrant(s) accordingly. Such changes will be available on the Registry Website or such other URL as the Registry may designate, which shall satisfy all notice requirements set forth in the Registry-Registrar Agreement. At any time after the notice period expires a user who accesses or uses the Registry Services will be bound by the effective Acceptable Use and Anti-Abuse Policy at that time.

PLEASE READ THIS POLICY CAREFULLY. BY ACCESSING OR USING THE REGISTRY SERVICES, YOU EXPRESSLY AGREE TO BE BOUND BY THE TERMS DESCRIBED HEREIN AND ALL TERMS INCORPORATED BY REFERENCE. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, YOU SHALL NOT ACCESS OR USE THE REGISTRY SERVICES.

REGISTRANT OBLIGATIONS

Each Registrant agrees:

1.1 Not to use the domain name in violation of any of the provisions of the Acceptable Use Policy.

1.2 To provide: (i) accurate and up-to-date WHOIS information, including contact information; and (ii) timely and accurate updates to WHOIS contact information.

1.3 By registering a domain name in the TLD, each Registrant represents (as/if required) that:

1.3.1 (if applicable) it possesses any and all necessary authorisations, accreditations, charters, licences and/or other related credentials necessary for participation in the regulated sector associated with the TLD and agrees to verification of same post registration.

1.3.2 (if applicable) it will continue to conform to the appropriate laws and regulations, including updates and renewals of any and all necessary authorisations, accreditations, charters, licences and/or other related credentials necessary for continued participation in the regulated sectors and/or activities indicated;

1.3.3 (if applicable) it will promptly report to its Registrar(s) any material changes to the validity of authorisations, accreditations, charters, licences and/or other related credentials provided at the time of registration and/or which affect such Registrant's continued participation in the regulated sector and/or activities indicated and associated with the Registry TLD.;

1.3.4 (if applicable) it will not claim or infer to have authorisations, accreditations, charters, licences and/or other related credentials that it does not possess;

1.3.5 it will provide and keep up-to-date an administrative contact, to be used by the Registry and/or the Registrar for the notification of complaints or reports of registration abuse; and

1.3.6 it will keep up-to-date information on the name and contact details of the regulatory, or industry self-regulatory entity or entities with control or jurisdiction over its main place of business, such information to be presented promptly upon request in cases where verification is necessary.

Each Registrant agrees:

1.4 To comply with all applicable laws and regulations, including those that relate to privacy, data collection, consumer protection (including in relation to misleading and deceptive conduct), fair lending, debt collection, organic farming, disclosure of data, and financial disclosures.

1.5 To implement reasonable and appropriate security measures, as defined by applicable law, if they collect and maintain sensitive health and financial data.

1.6 Not to upload, display, promote or otherwise distribute content for which they do not have a legal or contractual right.

1.7 Not to upload, transmit, display, promote or otherwise distribute any material in violation of any applicable law or regulation. This includes material that is:

1.7.1 harassing, bullying, abusive, and / or constitutes an illegal threat, violates export control laws, and hate propaganda; or

1.7.2 sensitive and proprietary or otherwise prohibited by local, national and or international industry regulations.

1.8 Not to infringe or otherwise interfere with the proprietary rights and or trademarks of other parties.

1.9 Not to claim, falsely state, infer, or otherwise misrepresent its affiliations.

1.10 Not to speak for, or on behalf of any individual, business, association, institution or other organization for which they have no authorisation.

1.11 Not to upload, display, promote or otherwise distribute content intended to defame, scorn, or ridicule, the Registry and/or its Affiliates and subsidiaries, nor its respective owners, directors, managers, officers, employees, contractors, service providers and/or agents.

1.12 Not to use private registration (Proxy Service) as means of providing anonymity in order to engage in unlawful or fraudulent activities including those meant to violate the

intellectual property rights of third parties.

2 ABUSE

The Registry defines abuse as an action that causes actual and substantial harm, or is a material basis of such harm, creates security and stability issues for the Registry, or is illegal, illegitimate, or otherwise contrary to registration policy. Abuse includes, without limitation, the following:

2.1 Where the domain name violates a third party's rights or acceptable use policies, including but not limited to the infringement of any copyright or trademark;

2.2 Content or actions that infringe the trademark, copyright, patent rights, trade secret or other intellectual property rights, or any other legal rights of IG Group, or any of its subsidiaries, or any third party;

2.3 Content that is in breach of a person's privacy rights or is otherwise in breach of any duty owed to a third party;

2.4 Content or actions that violate any applicable local, state, national or international law or regulation;

2.5 Content or actions that promote, are involved in or assist in, the conduct of illegal activity of any kind or promote business opportunities or investments that are not permitted under applicable law;

2.6 Content that advertises or offers for sale any goods or services that are unlawful or in breach of any national or international law or regulation; or

2.7 Content or actions associated with the sale or distribution of prescription medication without a valid prescription;

2.8 Content that is defamatory, or which otherwise may cause or incite injury, damage or harm of any kind to any person or entity;

2.9 Content which publicizes, displays, promotes or distributes child pornography;

2.10 Activities that mislead or deceive minors into viewing sexually explicit material;

2.11 Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums. An example, would be the use of email in denial-of-service attacks, distribution of phishing, malware or botnet attacks;

2.12 Phishing: The use of counterfeit Web pages that are designed to deceive recipients into disclosing sensitive data such as usernames, passwords, or financial data;

2.13 Pharming: The redirecting of unknowing users to fraudulent sites or services,:

2.14 Domain Name System (DNS) hijacking or poisoning;

2.15 Wilful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keyloggers, and trojan horses;

2.16 Botnet command and control: Services run on a domain name that are used to control a collection of illegally compromised computers or "zombies," or to direct denial-of-service attacks (DDoS attacks); and

2.17 Illegal Access to Other Computers or Networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures on another individual's system (often known as "hacking").

2.18 Any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information gathering activity).

The Registry provides an abuse point of contact through an e-mail address (currently: abuse@bostonivy.co). This e-mail address is used by the Registry to monitor and address abuse reports.

The AUP may be triggered through a variety of channels, including, among other things, private complaint, public alert, government or enforcement agency outreach, and the on-going monitoring by the Registry or its partners. In all cases, the Registry or its designees will alert the Registry's Registrar partners about any identified threats, and will work closely with them to bring offending sites into compliance.