Acceptable Use Policy

Overview

This Acceptable Use Policy (the **"Policy"** or **"AUP"**) applies to FoodChain ID (and its Affiliates) cloud services and Products including, without limitation, use of content, services, deliverables, and/or software licensed or sublicensed by FoodChain ID to you (collectively the **"Cloud Services"**). This Policy is incorporated into and forms part of the Master Services Agreement, Global Subscription and Services Agreement, Global Software Licensing Agreement, Terms of Use, Affiliate License Agreements, Data Usage Agreements or other similar agreement (the **"Agreement"**) between you and FoodChain ID Group, Inc., or its Affiliates (collectively **"FoodChain ID"**) for the provision of FoodChain ID Products and Cloud Services. Capitalized terms used but not defined herein have the meaning ascribed to them in the Agreement. "**Affiliate**" means a current or future entity that is controlled by, or is under common control with FoodChain ID Group, Inc.; "**FoodChain ID Group, Inc.**" means its affiliates and subsidiaries including Decernis, Nutraveris, Viaware, Hamilton Grant, Verdant, BCGlobal, Cosmocert, S.A., Lexagri International, and any subsequently acquired entities under the umbrella of FoodChain ID Group, Inc., collectively known as FoodChain ID. "**Cloud Services**" means hosted software applications provided as a service by FoodChain ID for use by a client.

This Policy prohibits uses and activities involving the Cloud Services that are illegal, infringe the rights of others, interfere with or diminish the use of the Cloud Services by other users, or otherwise adversely affect the Cloud Services or FoodChain ID. If you violate this Policy in any way, FoodChain ID may suspend or terminate your Agreement and your access to the Cloud Services.

In connection with using Cloud Services, you agree to ensure that all users (i) are notified that you have the right to monitor, access, record, report on, and otherwise create records regarding each user's use, logs, credentials, and access of the Cloud Services, and (ii) consent to the same. When you use the Cloud Services, you must not do any of the following:

1. **Conduct and information restrictions**

- Undertake any unlawful purpose, including, but not limited to, collecting, posting, storing, transmitting or disseminating information, data or material which is libelous, obscene, unlawful, threatening or defamatory, or which infringes the intellectual property or privacy rights of any person or entity, or which in any way constitutes or encourages conduct that would constitute a criminal offense, or otherwise violates any applicable local, state, provincial, federal, foreign, or other law, order, or regulation including, but not limited to those applicable to the client related to privacy, publicity, data protection, electronic communications and anti-spamming laws. You hereby represent you own or have the required rights to any data or information uploaded into the Cloud Services by you or your users or personnel;
- Obtain, access, export, transmit, move or copy any data, information or material for which you do not have adequate rights to take such action, or which was obtained using the Cloud Services for unlawful purpose;
- Use the Cloud Services for benchmarking, timesharing or service bureau purposes or otherwise for the benefit of a third party;
- Attempt, in any manner, to obtain the password, account, or other security information from any other user or log into a server or account on the Cloud Services that you are not authorized to access;
- Permit or allow any user sharing, distribution or group use of login information, including usernames or passwords;
- Upload, post, publish, transmit, reproduce, copy, create derivative works of, or distribute in any way information, software or other material obtained through the Cloud Services or otherwise that is protected by copyright or other proprietary right, without being the owner of such material or otherwise obtaining any required permission of the owner;

- Use any name, logo, tagline or other mark of FoodChain ID or its Affiliates, including without limitation: (a) as a hypertext link to any website or other location (except as provided for or enabled expressly by FoodChain ID in writing); or (b) to imply (i) support or endorsement by FoodChain ID and its affiliates of your activities or (ii) identification with FoodChain ID as an employee, contractor, agent or other similar representative capacity. You also agree not to remove or alter any of these items as FoodChain ID may have provided or enabled;
- Create any link to the Cloud Services or frame or mirror any content contained or accessible from the Cloud Services;
- Distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (e.g., spam);
- Participate in the collection of very large numbers of e-mail addresses, phone numbers, screen names, or other identifiers of others (without their prior consent), a practice sometimes known as scraping, spidering or harvesting, or participate in the use of software (including spyware) designed to facilitate this activity;
- Impersonate any person or entity, engage in sender address falsification, forge anyone else's digital or manual signature, or perform any other similar deceptive, misleading or fraudulent activity (e.g., "phishing"); and
- Use contact information or e-mail lists in a manner that is likely to result in an excessive number of unsubscribe requests or spam complaints or notices, as determined by acceptable industry practices.
- Upload any 1) patient, medical or other protected health information regulated by Health Insurance Portability and Accountability Act of 1996 (HIPAA) any similar federal or state laws, rules or regulations, 2) any social security numbers or payment card information, or 3) any "inside information" or "material non-public information" as defined by applicable law(s) (collectively 1), 2), and 3) **"High Risk Data"**). NOTWITHSTANDING ANYTHING IN THE AGREEMENT, A) CLIENT ACKNOWLEDGES AND AGREES THAT THE CLOUD SERVICES ARE NOT DESIGNED FOR HIGH RISK DATA AND UPLOADING HIGH RISK DATA AND USING THE CLOUD SERVICES IN CONJUNCTION WITH HIGH RISK DATA IS AT CLIENT'S OWN RISK; AND B) FOODCHAIN ID WILL NOT IN ANY WAY BE LIABLE FOR INACCURACIES, ERRORS, OMISSIONS, DELAYS, DAMAGES, CLAIMS, LIABILITIES OR LOSSES, REGARDLESS OF CAUSE, IN OR ARISING FROM HIGH RISK DATA OR ITS INCLUSION INTO THE CLOUD SERVICES.

2. **Technical restrictions**

- Use extreme bandwidth capacity in a way that threatens FoodChain ID's infrastructure or the ability of another user to access and use the Cloud Services;
- Upload viruses or malware or any other software, hardware device or code intended to harm or disrupt the Cloud Services;
- Attempt to overload the system with email or traffic;
- Use or distribute tools or devices designed or used for compromising security or whose use is otherwise unauthorized, such as password guessing programs, decoders, password gatherers, keystroke loggers, analyzers, cracking tools, packet sniffers, encryption circumvention devices, or Trojan Horse programs. Unauthorized port scanning is strictly prohibited;
- Distribute programs that make unauthorized changes to software (cracks);
- Alter, modify, or tamper with the Cloud Services or its security or permit any other person to do the same who is not authorized by FoodChain ID; or
- Attempt to probe, scan or test the vulnerability of the Cloud Services or to breach the security or authentication measures without proper authorization (e.g., agreement in writing with FoodChain ID's Chief Security Officer).

3. **Network and usage restrictions**

- Restrict, inhibit, or otherwise interfere with the ability of any other entity or individual, to use the Cloud Services, including without limitation (i) sending information in a way that is likely to be marked as spam or compromise the reputation of an IP address, and (ii) posting or transmitting any information or software which contains a worm, virus, or other harmful feature, or generating levels of traffic sufficient to impede others' ability to use, send, or retrieve information;

- Restrict, inhibit, interfere with, or otherwise disrupt or cause a performance degradation to the Cloud Services or any FoodChain ID (or FoodChain ID Affiliate or supplier) host, server, backbone network, node or service; or
- Interfere with computer networking or telecommunications service to any user, host or network, including, without limitation, denial of service attacks, flooding of a network, overloading a service, improper seizing and abusing operator privileges, and attempts to "crash" a host.

Changes to This Policy

FoodChain ID is constantly trying to improve the Cloud Services, so FoodChain ID may need to change this Policy from time to time. If FoodChain ID materially modifies this Policy, FoodChain ID will use commercially reasonable efforts to alert you to such modifications by placing a notice on the FoodChain ID website, the Cloud Services, by sending you an email, and/or by some other means. This Policy, as modified, will continue to govern your use of the Cloud Services. If you use the Cloud Services after any changes to this Policy have been posted, that means you agree to the changes.