Information Security Addendum

This Information Security Addendum ("ISA") sets forth the administrative, technical and physical safeguards Waterleaf International, LLC ("Waterleaf") takes to protect Confidential Information as part of its Information Security Program ("ISP"). Waterleaf may update this ISA from time to time to reflect changes in Waterleaf's ISP, provided such changes do not materially diminish the level of security herein provided. The provisions of this ISP apply to the Cyberleaf Cybersecurity-as-a-service Product Offering.

This ISA is made a part of your Cyberleaf General Terms and Conditions ("Agreement") with Waterleaf. Any capitalized terms used, but not defined herein, shall have the meaning set forth in the Agreement. In the event of any conflict between the terms of the Agreement and this ISA, the terms of this ISA will apply. This ISA does not apply to Third-Party Content purchased or acquired through Waterleaf.com or Cyberleaf.io, to any Evaluation or Free Software, or to any Extensions.

During the Term of the Agreement, Waterleaf agrees to maintain an ISP in conformance with the requirements set forth below.

Waterleaf's Information Security Program and Security Program Office

Waterleaf's ISP is reasonably designed to help protect the confidentiality, integrity, and availability of Confidential Information against any anticipated threats or hazards; unauthorized or unlawful access, use, disclosure, alteration, or destruction; and accidental loss, destruction or damage.

Waterleaf's ISP contains technical and organizational measures that are appropriate to: (i) the nature, size, and complexity of Waterleaf's business; (ii) the resources available to Waterleaf; (iii) the type of information that Waterleaf stores; and (iv) the need for security and confidentiality of such information.

Waterleaf's Chief Information Security Officer leads Waterleaf's ISP and develops, reviews and approves (together with other internal resources) Waterleaf Security Policies (as defined below).

Security Policies and Procedures

Waterleaf maintains information security, use and management policies (collectively "Security Policies") designed to educate employees and contractors regarding appropriate use, access to and storage of Confidential Information; restrict access to Confidential Information to members of Waterleaf's workforce who have a "need to know" such information; prevent terminated employees from accessing Waterleaf information and information systems post-termination; and imposing disciplinary measures for failure to abide by such policies. Waterleaf performs background checks of its employees at time of hire, as permitted by law. Where feasible and as applicable, Waterleaf endeavors to align its Security Policies to ISO 27001NIST, CIS, CMMC and other relevant level standards for information security.

Waterleaf Security Policies are available to employees via the company server. Waterleaf reviews, updates and approves Security Policies once annually to maintain their continuing relevance and accuracy.

Security Training and Awareness

New employees are required to complete security training as part of the new hire process and receive annual and targeted training (as needed and appropriate to their role) thereafter to help maintain compliance with Security Policies, as well as other corporate policies, such as the Waterleaf Code of Conduct. This includes requiring Waterleaf employees to annually re-acknowledge the Code of Conduct and other Waterleaf policies as appropriate. Waterleaf conducts periodic security awareness campaigns to educate personnel about their responsibilities and provide guidance to create and maintain a secure workplace.

Physical and Environmental Access Controls

Waterleaf limits physical access to its owned or leased information systems and facilities using physical controls (e.g., coded badge access) that provide reasonable assurance that access to its facilities and data centers is limited to authorized individuals and employs camera or video surveillance systems at critical internal and external entry points. All visitors must sign in and be escorted if in areas where sensitive data is accessible.

Waterleaf applies air temperature and humidity controls for its data centers and protects against loss due to power failure.

Logical Access Controls

Waterleaf employs monitoring and logging technology to help detect and prevent unauthorized access attempts to its networks and production systems. Waterleaf's monitoring includes a review of changes affecting systems' handling authentication, authorization, and auditing; and privileged access to Waterleaf production systems. Waterleaf uses the principle of "least privilege" (meaning access denied unless specifically granted) for access to customer data.

Threat and Vulnerability Management

As part of its Threat and Vulnerability Management Program ("TVM"), Waterleaf:

- Monitors for vulnerabilities in supported versions of the Software that are acknowledged by vendors, reported by researchers or discovered internally;
- Verifies vulnerabilities, rates them according to industry-standard ratings systems, and identifies them for mitigation or fixes based on severity level;
- Maintains patch management processes including mitigations or fixes in minor and major product releases, as part of its maintenance program, which may include cumulative fixes for certain vulnerabilities; and
- Makes reasonable efforts to expedite maintenance releases for supported versions that may be affected in the case of critical risk and high impact vulnerabilities.

The current version of Waterleaf Product Security Policy, if updated, which provides further detail on Waterleaf's TVM, is available at: https://cyberleaf.io/legal

Waterleaf regularly performs vulnerability scans and addresses detected vulnerabilities on a risk basis. Periodically, Waterleaf engages third-parties to perform network vulnerability assessments and penetration testing.

Incident Response Plan and Breach Notification

Waterleaf employs an incident response framework (the "Waterleaf Incident Response Framework" or "WIRF") to manage and minimize the effects of unplanned security events. The WIRF includes procedures to be followed in the event of an actual or potential security breach, including: (i) an internal incident response team with a response leader; (ii) an investigation team performing a root cause analysis and identifying affected parties; (iii) internal reporting and notification processes; documenting responsive actions and remediation plans; and (iv) a post-incident review of events.

For Customers located outside the US, Waterleaf provides notice without undue delay after becoming aware of a Data Breach. As used in this ISA, Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Personal Data as defined under the General Data Protection Regulation (EU) 2016/679 ("GDPR") while being transmitted, stored or otherwise processed by Waterleaf. If Customer reasonably determines notification is required under GDPR, Waterleaf will provide reasonable assistance to the extent required, including assistance in notifying the relevant supervisory authority and providing a description of the Data Breach.

For Customers located within the US, Waterleaf provides notice of a breach of Personal Information, as defined under the California Consumer Privacy Act of 2018 ("CCPA"), as required under California law.

Storage and Transmission Security

Technical security measures to guard against unauthorized access to Customer data that is being transmitted over a public electronic communications network or stored electronically.

Secure Disposal

Policies and procedures regarding the disposal of tangible and intangible property containing Customer Confidential Information so that wherever possible, Customer Confidential Information cannot be practicably read or reconstructed.

Risk Identification and Assessment

Waterleaf employs a risk assessment program to help it reasonably identify foreseeable internal and external risks to Waterleaf's information resources and determine if its existing controls, policies, and procedures are adequate to address the identified risks.

Secure Development

Waterleaf's Software Development Life Cycle ("SDLC") methodology governs the acquisition, development, implementation, configuration, maintenance, modification, and management of internally developed software components.

For major product releases, Waterleaf uses a risk-based approach when applying its standard SDLC methodology, which may include such things as performing security architecture reviews, open-source security scans, dynamic application security testing, network vulnerability scans and external penetration testing in the development environment. Waterleaf performs security code review for critical features if needed; and performs code review for all features in the development environment.

Waterleaf scans packaged software to verify it's free from trojans, viruses, malware and other malicious threats.

Waterleaf utilizes a code versioning control system to maintain the integrity and security of application source code. Access privileges to the source code repository are reviewed periodically and limited to authorized employees.

As noted above, this ISA, including its SDLC methodology, does not apply to any Extensions (Customer's or Waterleaf's) or to Third- Party Content, including any made available on cyberleaf.io.

Vendors

Third-party vendors (collectively, "Vendors") with access to Confidential Information are subject to contractual obligations of confidentiality and risk assessments to gauge the sensitivity of information being shared. Vendors are expected to comply with any pertinent contract terms relating to the security of data, as well as any applicable Waterleaf policies or procedures. Periodically, Waterleaf may ask the Vendor to re-evaluate its security posture to help ensure compliance.