HackedAlert Terms and Conditions (v1.0)

1. Objective and Scope

HackedAlert is a technical intelligence (OSINT) platform, whose objective is to provide access to information (data and metadata) indexed and collected from open sources.

HackedAlert processes and serves a large amount of information from publicly accessible sources; the platform acts as a search engine that is agnostic toward technologies and the market in general.

2. Nature and Processing of Information

All information contained and served on the platform is in the public domain. However, data and metadata are processed, categorized, correlated, and enriched with relevant industry intersections to facilitate their consumption, understanding, and commercial or technical reuse.

- **Origin of Data**: We do not store, process, or facilitate access to information originating from illicit acts, data leaks, cybersecurity attacks, or any type of data or metadata of criminal origin.
- **Indexing Methodology**: HackedAlert limits itself exclusively to indexing technical metadata that is voluntarily and openly exposed by the systems indexed to the Internet. The platform does not perform authentication attempts, does not exploit vulnerabilities, and does not bypass access control mechanisms (such as firewalls, authentication systems, or end-to-end encryption) to obtain the indexed information.
- **Fidelity of Result**s: To guarantee compliance with current legislation, no autonomous or unilateral activity is performed (neither before, during, nor after storing and serving information from the platform) to technically verify the scientific fidelity of the results obtained from reconciliation. Therefore, it is probable that data and metadata may contain errors, inaccuracies, or temporary obsolescence.
- **CVE Identifiers and Pentesting**: The platform does not execute pentesting procedures or any other activity related to the reproduction of computer vulnerabilities or CVE identifiers, nor does it provide tools, code, or programs to test CVE identifiers or perform pentesting. The classification and correlation of information with CVE identifiers has an exclusively informative purpose and is intended to provide visibility into the technical exposure surface. This functionality does not constitute a means to facilitate illicit access, as it does not provide exploits or execution tools, limiting itself to reporting vulnerability information widely disseminated in public security databases.

- **Exclusion of Technical Responsibility**: Since we do not verify the technical authenticity of the data and metadata by design, the platform is provided "as is".

3. Privacy and Personal Data

HackedAlert operates under a privacy and security by design model, limiting its data collection strictly to technical information of publicly exposed infrastructure, excluding the collection of personal data that is not strictly necessary for the technical identification of the asset. HackedAlert implements technical procedures intended for the anonymization of personal data when appropriate, guaranteeing that the storage, processing, and disclosure of data and metadata are strictly limited to public technical infrastructure information, and not to sensitive or private personal data.

- **IP Addresses**: In compliance with Article 11, paragraph j) and Article 27 of Law No. 21.663, the processing of IP addresses performed by the platform is limited exclusively to their technical function as a network identifier, and they are not treated under the category of personal data for the purposes of this regulation.
- **Domain Assets**: Likewise, in accordance with the technical and operational nature of domain names, it is declared that any asset registered under the .cl TLD, as well as those linked to public bodies (.gob.cl, .gov.cl, .mil.cl) and any other generic or territorial TLD, together with their associated subdomains, constitute public assets; such elements are managed under the rules of assignment and registration of domain names, being public information by their very operational nature. Consequently, the processing, indexing, and correlation of such domain names and their hierarchical structures (subdomains) does not constitute personal data processing, as it does not link, refer to, or allow the identification of a natural person, thus being excluded from the scope of Law No. 19.628 and its current modifications (Law No. 21.719).

4. ARCOP Rights and Transparency

In compliance with Law No. 21.719, HackedAlert recognizes the right of data subjects to exercise the powers of Access, Rectification, Cancellation, Opposition, and Portability (ARCOP). Users or data subjects whose (identifiable) personal data might be indexed and available for consultation in HackedAlert search results may exercise these rights by sending a request to contacto@wl-inc.cl, in accordance with the procedure established in Article 11 of Law No. 19.628 (as amended).

5. Responsible Use and User Obligations

The use of the platform and its information for purposes that contravene Law No. 21.459, Law No. 21.663, Law No. 21.719, Law No. 19.628, or any other legislation or regulation in force in Chile, makes the end user exclusively responsible for the use made of the intelligence obtained through HackedAlert.

- **Critical Infrastructure**: It is strictly prohibited to use HackedAlert for the purpose of identifying, enumerating, or analyzing infrastructure of public utility services or critical assets defined under the Cybersecurity Framework Law (Law No. 21.663) for the execution of attacks or interruptions. HackedAlert declines all responsibility for the unauthorized use of its information to affect such strategic services. HackedAlert is not designed exclusively for the monitoring or surveillance of critical infrastructures or essential services defined in Law No. 21.663, and any query made regarding such assets must be executed in strict compliance with the sectoral cybersecurity obligations that apply to the user.
- **Purpose of Processing**: The processing performed by HackedAlert has the exclusive purpose of technical asset analysis and security research (OSINT), within the framework of a legitimate interest to provide visibility into the public attack surface, and such data shall not be used for marketing purposes, profiling of natural persons, or the creation of profiles.

6. Collaboration with the Authority and Protocols

- **Legal Cooperation**: HackedAlert will always collaborate with authorities and the police in cases of cybercrime related to the abuse or misuse of the platform and its content.
- **Response to Vulnerabilities**: If users or third parties inform HackedAlert about the detection of vulnerabilities, HackedAlert reserves the right to act in accordance with the principles of responsible disclosure, and may, at its discretion, channel such information to the owners or managers of the affected systems, as well as to State institutions as appropriate, without this constituting an assumption of responsibility for the veracity of the finding.
- **Legal Positioning**: HackedAlert does not act under the "responsible disclosure of vulnerabilities" regime provided for in Article 2 of Law No. 21.459, as it does not perform intrusive scanning or vulnerability testing. Consequently, HackedAlert does not position itself as a security research entity subject to the obligations of that body of law, but rather as a public information indexing service.

- **Exclusion Management**: HackedAlert acts as a search engine for publicly accessible data. Given the dynamic and constant nature of indexing open sources, the platform does not guarantee the permanent elimination of assets, as these may be automatically re-indexed in future processes. However, HackedAlert respects standard industry technical protocols (such as robots.txt files or noindex meta-tags), which are the recognized technical mechanism for system administrators to express their will not to be indexed by crawlers or bots. The implementation and maintenance of such technical measures are the exclusive responsibility of the system administrator. HackedAlert does not offer asset management, cleaning, or auditing services to third parties, nor does it provide technical consulting services for data exclusion.

7. Subscription Plans

- **Consumption Plans**: HackedAlert offers subscription plans which can be paid via bank transfer, deposit, or online with automatic charges to credit and debit cards.
- **Plan Features**: HackedAlert reserves the right to add, remove, or modify subscription plans, plan features, and service scopes on the platform, unilaterally and without prior notice.
- **External Payment Gateway**: HackedAlert uses the payment gateway service provided by MercadoPago; however, this provider may be replaced at any time and without prior notice.

8. Contact

For any questions or requests, you may contact our team using the following email address: contacto@wl-inc.cl.

Santiago, Chile, May 26, 2026.