IRONCHIP
CYBERSECURITY

General Terms and Conditions of Software License

Identity Platform and Mobile Application

Your Next Generation Identity

Table of Contents

This document sets forth the general terms and conditions governing the license for the use of IRONCHIP's software solutions, including the identity platform and, where applicable, the associated mobile applications (hereinafter, collectively referred to as the "Software" or the “Licensed Solution”), as well as the related services (hereinafter, the “Services”) provided by **IRONCHIP TELCO, S.L.** (hereinafter, "IRONCHIP") to the client who contracts and uses said Software and Services (hereinafter, the "Client").

Acceptance of these General Terms and Conditions for the Software License is an essential requirement for accessing and using IRONCHIP’s Software, whether through web environments, mobile or desktop applications, email, USB tokens, NFC/RFID cards, or delegated authentications.

1.-DEFINITIONS

For the purposes of these Terms and Conditions, the following terms shall have the meanings set forth below:

- **Client:** The entity or legal person that acquires a license to use IRONCHIP's Software and/or contracts the associated Services.
- **Subscription Agreement:** The specific agreement entered into between IRONCHIP and the Client that details the commercial, economic, and particular conditions of the Subscription and the Services, including scope, duration, and applicable fees. These General Terms and Conditions form an integral part of the Subscription Agreement.
- **Documentation:** Any manual, guide, technical specification, or reference material provided by IRONCHIP in relation to the Software and/or the Services.
- **Confidential Information:** Any information or documentation owned by or belonging to either Party which, although not public in nature, is exchanged or accessed in any form or medium within the context of their relationship, provided it is designated as confidential or should reasonably be understood as confidential by the nature of the information. This includes, but is not limited to, trade secrets, financial and business information, personal data, technical specifications and information about products and technologies, passwords, know-how, and internal procedures.
- **License:** The non-exclusive and non-transferable right granted by IRONCHIP to the Client to use the Software in accordance with these Terms and Conditions and the Subscription Agreement.
- **Parties:** Jointly refers to IRONCHIP and the Client.
- **Services:** The services related to the Subscription and the Software, including support, maintenance, and any other service specified in the Subscription Agreement.
- **Third-Party Services:** Products, services, networks, infrastructures, APIs, platforms, or components provided by third parties external to IRONCHIP (including but not limited to email service providers, telecommunications operators, SMS and push notification providers, cloud services, SIEM systems, authentication tools, or external integrations) with which the Software may interoperate or on which it may depend, directly or indirectly, for its operation. The use of Third-Party Services may be subject to terms

and conditions, usage policies, technical limitations, or fees established by such third parties, and the Client shall be responsible for compliance with them.

- **Software (or Licensed Solution):** The cybersecurity and digital identity applications or technological solutions owned by IRONCHIP that are provided to the Client under license/Subscription, including (i) the identity platform accessible via web and/or API, and (ii) the associated mobile applications that allow Authorized Users to authenticate or interact with such platform. The Licensed Solution includes any improvement, update, or adaptation thereof. The specific functionality will depend on the license edition acquired by the Client (e.g., Free, Enterprise, Premium) and the configuration established in the Subscription Agreement and applicable Documentation.
- **Subscription:** The right to access and use IRONCHIP's Software under the SaaS (Software as a Service) model for a determined period and subject to the payment of the corresponding fees.
- **Authorized User:** Any employee, contractor, or agent of the Client authorized by the Client to access and use the Software on its behalf, in accordance with the terms of the License.

2.- PURPOSE AND SCOPE OF THE LICENSE

2.1. The purpose of this document is to establish the general terms and conditions applicable to the License for use of IRONCHIP Software and the provision of the associated Services.

2.2. **Permitted Use:** IRONCHIP grants the Client a non-exclusive and non-transferable License to use the Licensed Solution solely for internal business purposes of the Client during the term of the corresponding Subscription and subject to the terms and payment of the fees set forth in the Subscription Agreement. The specific functionality of the Software will depend on the license edition acquired by the Client and the limitations specified in the applicable Documentation.

2.3. **Usage Restrictions and License Usage Verification:** The Client shall refrain from performing, or allowing third parties to perform, the following actions without the prior written authorization of IRONCHIP:

1. Assigning, reselling, sublicensing, leasing, lending, distributing, publicly communicating, commercially exploiting, or transferring the License or the Software to third parties.
2. Modifying, interfering with, or tampering with the Licensed Solution, as well as performing any act that circumvents or manipulates potential restrictions or security or control measures installed in it.
3. Attempting to probe, investigate, explore, or test the vulnerability of the Licensed Solution or IRONCHIP's IT systems, or attempting to disassemble, decrypt, or disable any security or control measure or system related to the Licensed Solution or to the systems or technologies on which it operates.
4. Using the Software in any way that infringes IRONCHIP's or third parties' intellectual property rights.

5. IRONCHIP may, with reasonable prior notice and a minimum of five (5) business days' notice, remotely and/or through documentation verify that the Client's use of the Software complies with the terms of the License and the conditions of the Subscription Agreement, including but not limited to the number of Authorized Users, active devices, integrations, volumes of authentications, or any other parameter applicable to the licensed model contracted. For this purpose, the Client shall cooperate by providing the information reasonably required for such verification, including logs, screenshots, configurations, or reports generated by the Software. In case of overuse, the Client must immediately regularize the situation by acquiring the corresponding additional licenses and paying the applicable fees. Performing these verifications shall not grant the Client any right of access to IRONCHIP's source code, infrastructure, or internal systems.

2.4. **Immediate Suspension for Security or Unlawful Use:** IRONCHIP may immediately suspend, in whole or in part, the access of the Client or any of its Authorized Users to the Software, without prior notice, when it has reasonable grounds to believe that:

a) the use of the Software is or may be unlawful, contrary to applicable regulations or to these Terms and Conditions;
b) there is a real or potential risk to the security, integrity, availability, or proper functioning of the Software, IRONCHIP's infrastructure, or that of other clients;
c) the Client or an Authorized User has seriously breached the Acceptable Use Policy, the Usage Restrictions set out in Clause 2.3, or any essential obligation arising from these Terms;
d) access to or use of the Software may result in legal, regulatory, or compliance liabilities for IRONCHIP or affect third parties;
e) there are reasonable indications of unauthorized access, credential compromise, fraudulent activities, attacks, exploitation of vulnerabilities, or any malicious activity.

Suspension under this clause shall not entitle the Client to any compensation, refund, penalty, or indemnity. IRONCHIP will restore access when the risk or cause of suspension has ceased and the Client has reasonably demonstrated remediation of the conduct that triggered the suspension.

2.5. **Acceptable Use Policy for the Software and Services:** The Client and its Authorized Users agree to use the Software and Services in accordance with this Acceptable Use Policy ("AUP"), any breach of which shall entitle IRONCHIP to suspend, in whole or in part, access to the Software or Services immediately, without prejudice to any other legal actions that may apply.

a) Unlawful or Unauthorized Activities: The Client shall not, directly or indirectly, use the Software or the Services to:

1. **Engage in activities that contravene applicable laws**, including, but not limited to, fraudulent or criminal acts, privacy violations, intellectual property infringements, identity theft, or unauthorized access to systems or data.
2. **Distribute, store, transmit, or execute illegal**, defamatory, offensive, discriminatory content or any content that infringes third-party rights.

3. Use the Licensed Solution to support third-party **services that compete with IRONCHIP** or to develop derivative products or engage in reverse engineering of the Software.

b) Abuse of Service Security or Integrity: It is expressly prohibited to:

1. Upload, transmit, distribute, or facilitate malicious software, ransomware, spyware, trojans, viruses, or any code or instruction designed to damage, interfere with, intercept, or misappropriate systems, data, or communications.
2. Attempt **to probe, scan, investigate, or test vulnerabilities** in the Software, IRONCHIP's infrastructure, or third-party systems without prior written authorization from IRONCHIP.
3. Carry out denial-of-service (DoS) attacks, brute force attacks, access automation, token manipulation, privilege escalation, or any activity intended to compromise or bypass authentication or access control mechanisms.
4. Interfere with or attempt to interfere with the proper delivery of the Software, including the use of automated tools, bots, scripts, or mass access that degrade the quality or availability of the Services.

c) Improper Use of the Identity Platform: The Client shall not:

1. Manipulate identity validations, authentications, risk signals, location data, behavioral patterns, or any elements intended to ensure the security of the platform.
2. Use fake accounts, identities, or credentials, impersonate users, or allow shared access between multiple users.
3. Alter, modify, or falsify signals sent from devices, sensors, networks, or third-party integrations.

d) Abuse of Integrations and Third-Party Services: The Client understands and accepts that the Software relies on third-party services such as telecommunications operators, SMS providers, email, cloud infrastructure, SIEM services, etc.

It is prohibited to:

1. Use such integrations in a way that exceeds reasonable technical limits or the terms imposed by those third parties.
2. Execute mass automation or intensive use of APIs that may affect other clients or the stability of the service.
3. Reconfigure, manipulate, or misuse SMS, email, or push notification systems for purposes unrelated to authentication or the flows provided in the Documentation.

e) Protection of Platform Reputation and Security: The Client and its Authorized Users shall not:

1. Use the Software in a way that may create reputational, legal, or regulatory risk for IRONCHIP.
2. Attempt to register or use trademarks, domains, or names similar to IRONCHIP that may cause confusion.

3. Publicly disclose vulnerabilities or technical information about the Software without complying with IRONCHIP's responsible disclosure policy.

f) Client's Obligation to Monitor Use: The Client shall be solely responsible for:

1. Monitoring the use of the Software by its Authorized Users.
2. Adopting reasonable internal measures to ensure compliance with this AUP.
3. Immediately notifying IRONCHIP of any misuse, suspected abuse, security breach, or incident involving keys, tokens, or credentials.

g) Corrective Measures: IRONCHIP may, without prior notice, suspend or restrict access to the Software and Services when:

1. There is unlawful, fraudulent, or abusive use.
2. The behavior of the Client or its Authorized Users poses a real or potential risk to the security, privacy, or integrity of the platform or other clients.
3. There is a serious or repeated breach of this AUP.

Suspension shall not exempt the Client from its payment obligations nor entitle it to any refund.

2.6 **License Models:** The scope of the Subscription and Services will vary depending on the license model contracted by the Client and may include the following additional functionalities:

Enterprise Edition

Frictionless security and essential control

- **Passwordless identity and access management.** Secure passwordless or traditional authentication, at the client's discretion, for users and devices, minimizing the risk of credential theft.
- **Multiple access methods.** Compatibility with mobile and desktop applications, email, USB tokens, NFC/RFID cards, and delegated authentications.
- **Custom conditional access.** Granular configuration based on attributes such as device type, geographical location, identity composition, roles, or contextual risk level, effectively applying the Zero Trust principle.
- **Basic location detection.** Location intelligence applied to IP blocking via whitelists, secure zone management/creation, and contextual analysis of multiple locations.
- **Simple governance and permissioning.** User, group, and device management, with CSV exports or real-time synchronization with Active Directory (SCIM).
- **Standard integration.** Easy onboarding through direct integration with the most common identity management systems:
- Active Directory
- LDAP
- SCIM for Entra ID
- Google Cloud Identity
- CSV for local users
- **Centralized control panel.** Full real-time visualization of users, devices, accesses, and events, with extended metrics and traceability.

- **Audit & Compliance Reporting.** Functionality for regulated environments. Generates detailed reports, event logs, and full traceability, essential for audits and compliance with frameworks such as ENS, PSD2, DORA, or NIS2.
- **Customizable Look & Feel.** Adaptation of authentication flows to corporate design in applications, IDPs, or OS login screens.
- **Support**. Includes standard online support and automatic updates.

Premium Edition

Comprehensive security: Real-time fraud detection, forensic capabilities, and compliance

- **Passwordless identity and access management.** Secure passwordless or traditional authentication, at the client's discretion, for users and devices, minimizing the risk of credential theft.
- **Advanced Location Intelligence with Continuous Learning (AI).** Goes beyond static zone limitations. The system learns from users' typical behavior and location patterns to detect geographic anomalies in real time (e.g., access from an unusual location), applying contextual risk management.
- **Custom and Adaptive Fraud Detection Engine.** Implementation of custom business rules to identify specific fraud patterns (e.g., unusual transactions or changes to sensitive settings), adapting to each client's use case.
- **Forensics & Evidence Export (Forensic Analysis).** Dedicated forensic analysis tab that centralizes all information on a security event, allowing for the export of fraud evidence and full traceability for legal or compliance processes.
- **Real-Time User and Device Management.** Ability to instantly release or block compromised users or devices, ensuring an immediate response to active threats.
- **Advanced Customizable and Granular Access Policies.** Allows for the definition of complex access rules based on roles, user profiles, device types, location, or contextual risk level, effectively implementing the Least Privilege principle (Zero Trust).
- **SIEM Integration.** Export of access logs and security events via standard Syslog protocol or API, enabling basic ingestion into any SIEM system.
- **Real-Time Detection and Blocking (Rule-Based).** Ability to automatically detect and block access or actions that violate established business rules and access policies.
- **Instant Administrator Notification.** Sending of detailed and prioritized security alerts to administration teams upon any high-risk access attempt or blocking incident.
- **24/7 Premium Support and Ongoing Advisory.** Dedicated, uninterrupted support and a proactive advisory service for the ongoing development of new fraud rules and use cases.

2.7. **Free Services, Trial Versions and Testing:** IRONCHIP may offer the Client access to certain Software functionalities free of charge, in the form of a proof of concept (PoC), pilot, demo, sandbox, or evaluation (collectively, the "Free Services" or the "Trial Versions"). The Free Services are provided exclusively for the Client's internal evaluation purposes, without any obligation to continue with a Subscription or any right of the Client to demand specific functionalities, maintenance, support, or features equivalent to the paid editions.

The Free Services and Trial Versions are offered **"AS IS" and "AS AVAILABLE"**, without warranties of any kind, either express or implied, including but not limited to warranties of availability, service continuity, accuracy, error-free operation, fitness for a particular purpose, or non-infringement. IRONCHIP shall not provide SLAs, service credits, indemnities, or compensation in relation to the Free Services or Trial Versions.

IRONCHIP may modify, limit, suspend, or withdraw the Free Services or Trial Versions at any time, at its sole discretion and without prior notice. The Client acknowledges and agrees that any data uploaded, generated, or processed during the use of the Free Services may be deleted or become inaccessible upon their termination or suspension.

The Client shall be fully responsible for complying with these Terms and Conditions during the use of the Free Services or Trial Versions, including the Acceptable Use Policy, the technical restrictions of the License, and any applicable regulations.

2.8. **Official Documentation:** To obtain complete and detailed information about the IRONCHIP identity platform, including its various modules, functionalities, and user guides, the Client may consult the official documentation available at: https://docs.ironchip.com/

2.9. The License is granted for the Subscription Period agreed upon in the Subscription Agreement and is subject to the timely payment of the applicable fees.

2.10. The use of the Software and the provision of the Services shall be governed by these General Terms and Conditions, supplemented by any specific conditions included in the Subscription Agreement. In the event of a conflict between the general and specific conditions, the latter shall prevail.

2.11. Access to and use of the Software, including the mobile app, desktop application, email, USB tokens, NFC/RFID cards, and delegated authentications, shall require the express acceptance of these Terms and Conditions by the Client and, where applicable, by the Authorized Users. IRONCHIP or the Client, depending on the implementation architecture, may record the date, time, and version of the accepted Terms and Conditions, as well as other technical data associated with such acceptance, for the purpose of maintaining evidence of regulatory and contractual compliance.

3.- INTELLECTUAL AND INDUSTRIAL PROPERTY

3.1. IRONCHIP is and shall remain the sole holder of all intellectual and industrial property rights related to its trademarks, patents, inventions, technologies, software programs, computer applications, Documentation, know-how, algorithms, programming, source code, and any other elements it may have created or owns, including any improvements, adaptations, modifications, or derivative versions made thereto.

3.2. The License granted to the Client does not in any way imply the transfer of ownership or title of any of IRONCHIP's intellectual or industrial property rights to the Client. The Client only acquires a limited right to use the Software in accordance with the terms of the License.

3.3. The Client shall refrain from performing, or allowing third parties to perform, the following actions without IRONCHIP's prior written authorization:

1. Deciphering, decompiling, disassembling, reverse engineering, or attempting to discover the algorithms, programming, or source code of the Software with the aim of copying, developing, or obtaining an analogous or similar technology.
2. Performing or authorizing modifications, adaptations, or successive or derivative versions of the Software.

3.4. The Client's failure to comply with the obligations set forth in this Clause shall entitle IRONCHIP to immediately terminate the License, without prejudice to any other legal actions that may apply depending on the nature of the breach, and without exempting the Client from the payment of amounts already invoiced or pending invoicing under this Agreement.

4.- OBLIGATIONS OF THE PARTIES

4.1. **Obligations of IRONCHIP:**

1. Provide the Services diligently and professionally, in accordance with the required quality standards.
2. Provide assistance and technical support as detailed in Clause 10 (Maintenance and Support).
3. Inform the Client of any unforeseen events that may impact or require modifications to the content and scope of the contracted Services, and attempt to resolve any incidents arising as a result of such modifications.
4. Assist the Client in complying with obligations regarding digital operational resilience, supply chain security, and incident notification, to the extent required by regulations such as NIS2 or DORA, and provide the necessary documentation and cooperation for the Client's regulatory audits.

4.2. **Obligations of the Client:**

1. Pay the amounts invoiced by IRONCHIP for the Subscription and the contracted Services, in accordance with the terms established in the Subscription Agreement.
2. Allocate the necessary internal personnel and provide the information or documentation required by IRONCHIP for the proper delivery of the Services.
3. Refrain from using IRONCHIP's know-how or Confidential Information for any purpose outside the scope and purpose of the License and the Services.
4. Provide the necessary cooperation and support for the proper execution of the Services, including participation in agreed training sessions for Level 1 support.

5. Ensure that its Authorized Users comply with these Terms and Conditions and with all applicable laws and regulations regarding the use of the Software.
6. Maintain the confidentiality of the access credentials to the Software and be responsible for all activities occurring under its account.
7. The Client shall be fully and exclusively responsible for the use of the Software and Services by its Authorized Users, as well as by any affiliate, provider, subcontractor, consultant, or third party to whom the Client grants, directly or indirectly, access to or use of the Software, whether on a temporary or permanent basis. The Client shall ensure that such third parties comply at all times with these Terms and Conditions, and shall be liable to IRONCHIP for any breach, negligent action, improper access, unauthorized use, or violation of the License committed by them.

4.3. **Common Obligations:**

1. Comply at all times with their respective legal obligations, including but not limited to data protection and tax obligations.
2. Cooperate in all tasks or matters related to the Services.
3. Comply with the duty of confidentiality set forth in Clause 5.

4.4. In the event of the Client's breach of any of its obligations, IRONCHIP may temporarily suspend the provision of the Services and access to the Software until such breach is remedied, without this exempting the Client from the payment of invoiced or pending amounts.

5.- CONFIDENTIALITY

5.1. Both Parties mutually agree to treat as confidential the Confidential Information received from the other Party under or in connection with the contractual relationship.

5.2. The Receiving Party of the Confidential Information agrees to:

1. Not disclose or reveal any Confidential Information to third parties without the prior written authorization of the Disclosing Party.
2. Refrain from using the Confidential Information for any purpose or activity unrelated to the purpose of the License and the Services.
3. Take the reasonably necessary measures to preserve the Confidential Information, applying at least the same degree of diligence as it uses for the protection and safekeeping of its own confidential information.
4. Ensure that the Confidential Information is only accessed by employees, directors, collaborators, and other persons under its responsibility who reasonably need access to it for tasks or matters related to the License and the Services, and under the appropriate duties of confidentiality.
5. Inform its employees and other collaborators about the confidential nature of the Confidential Information and ensure compliance with their obligations.

6. Return or destroy the Disclosing Party's Confidential Information upon termination of the License, after prior notice, without prejudice to the fact that the confidentiality obligation shall survive its termination.

5.3. The following shall not be considered Confidential Information: (a) information that is in the public domain at the time of disclosure or subsequently becomes public knowledge through no fault of the Receiving Party; (b) information that has been independently developed without the use of the Disclosing Party's Confidential Information; (c) information that was lawfully in the possession of the Receiving Party prior to its disclosure by the Disclosing Party; or (d) information that must be disclosed by virtue of a legal provision, court order, or requirement of competent authorities, provided that such disclosure is limited strictly to the Confidential Information that is strictly necessary.

6.- PERSONAL DATA PROTECTION

6.1. Both Parties undertake to comply with their respective obligations and duties regarding the processing of personal data under their responsibility or control, in accordance with Regulation (EU) 2016/679 (GDPR) and Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), as well as any other applicable data protection regulations.

6.2. In cases where the Client acts as the Data Controller, the Client shall be solely responsible for ensuring the lawfulness of the personal data processing carried out through the Software, including, among others, obtaining the appropriate legal basis; providing information to data subjects; managing consents where applicable; determining the purposes and means of the processing; and the proper configuration, parameterization and use of the Software in accordance with applicable regulations. IRONCHIP shall not assume any liability arising from the Client's failure to comply with its obligations as Data Controller, nor from any regulatory, sanctioning or economic consequences resulting from such failure.

6.3. With regard to personal data processed through the identity platform and mobile application, IRONCHIP shall apply the technical and organizational measures defined in its Information Security and Privacy Management System, in accordance with applicable regulations and standards such as ISO/IEC 27001 and ISO/IEC 27701.

6.4. In the event that IRONCHIP must process personal data for which the Client is the controller in the context or as a consequence of the provision of Services, IRONCHIP shall act as Data Processor on behalf of the Client and solely for the purpose of providing the services under the Subscription Agreement, in accordance with the Data Processing Agreement formalized as Annex A to these Terms and Conditions. Said Annex A, and the commitments contained therein, form an integral and essential part of the Subscription Agreement, including the specification of the Client's data geographical location and the international transfer mechanisms used by IRONCHIP to ensure compliance with the GDPR.

6.5. The Parties mutually inform each other that the personal data of the signatories or representatives provided as a result of the contractual relationship will be included in a file owned by the other contracting Party for the purpose of maintaining, fulfilling, developing, monitoring, and executing the provisions of this agreement. Data subjects may exercise their rights of access, rectification, erasure, objection, restriction of processing, data portability, and not to be subject to automated individual decisions by means of written communication to the other Party.

6.6. **Priority of the Data Processing Agreement (DPA):** In cases where IRONCHIP processes personal data on behalf of the Client as Data Processor, such processing shall be governed exclusively by the provisions of the Data Processing Agreement attached as Annex A to these Terms and Conditions. In the event of any conflict, contradiction, or discrepancy between the provisions of this Section 6 and those of Annex A, the provisions of Annex A shall always prevail, as it is the specific instrument governing personal data processing in accordance with Article 28 of the GDPR.

6.7. **Deletion or Anonymization of Client Data:** Upon termination of the Subscription Agreement, for any reason, IRONCHIP shall delete or anonymize the Client's data processed through the Software once the retention period established in the Data Processing Agreement (Annex A) has elapsed, unless a legal obligation requires its retention for a longer period. IRONCHIP shall not be obligated to retain, store, or return any data that the Client has not exported within the established timeframe, and it shall be the Client's sole responsibility to safeguard and recover its own information before the effective termination date.

7.- SCOPE AND LIMITATION OF LIABILITY

7.1. The Services provided by IRONCHIP are of a technical nature and shall in no case replace the Client in acts of direction, management, and/or decision-making inherent to its own activity or related to tasks or actions for which it is responsible. The Client acknowledges and agrees that compliance with NIS2, DORA, and any other applicable sector-specific regulations is the sole responsibility of the Client, and that IRONCHIP's Software constitutes only a supporting element within its overall compliance framework. IRONCHIP shall not be liable for the Client's failure to comply with such regulatory obligations, nor for any penalties, corrective measures, or damages arising therefrom.

7.2. IRONCHIP warrants that, during the Subscription Period: (i) the Software will substantially conform to the specifications contained in the applicable Documentation; and (ii) IRONCHIP will provide the Services in a professional manner and in accordance with industry standards. The Client's sole remedy for any breach of this warranty shall be the correction or remediation of the error by IRONCHIP within a commercially reasonable timeframe or, if correction is not possible, the termination of the Subscription Agreement, the effects of which shall be governed by the provisions of the Term and Termination Clause.

7.3. Except for the warranties expressly stated in Clause 7.2, and to the maximum extent permitted by applicable law, IRONCHIP expressly disclaims and excludes all other warranties,

whether express or implied, statutory or otherwise, including but not limited to implied warranties of merchantability, fitness for a particular purpose, satisfactory quality, title, and non-infringement. The Software is provided "AS IS" and "AS AVAILABLE".

7.4. IRONCHIP shall only be liable for direct damages or losses that may be caused to the Client in connection with the defective performance of its work, provided they are the result of negligent acts or omissions attributable to IRONCHIP or its personnel. Any indirect, incidental, or consequential damages are expressly excluded, including but not limited to loss of profit, loss of data, business interruption, or loss of reputation.

7.5. IRONCHIP's maximum aggregate liability to the Client for any claim arising out of or related to these Terms and Conditions or the Subscription Agreement shall in no event exceed the annual amount paid by the Client to IRONCHIP in connection with the Subscription during the last annual period of the current Subscription. This limit shall apply regardless of the cause of the claim, the type of damage alleged, or the theory of liability invoked (including contractual, non-contractual, negligence, statutory breach, or otherwise). The limit shall be cumulative for all claims the Client may bring jointly or separately. This limit shall not apply to (i) the Client's payment obligations under the Subscription Agreement, or (ii) the indemnification obligations assumed by the Client under Clause 8.4.

7.6. The Client understands and agrees that IRONCHIP shall not be liable to the Client or any third party for any damage or loss arising from any incident, malfunction, or unavailability affecting the Software when such issues result from events or circumstances beyond IRONCHIP's control and responsibility, such as:

- Interruptions, errors, incidents, unavailability, or discontinuities related to the Client's or its end users' computer systems, equipment, devices, software programs, networks, servers, connectivity systems, or applications (including those resulting from inadequate configuration or lack of updates) or provided or operated by third parties unrelated to IRONCHIP.
- Incidents, outages, suspensions, or failures affecting the power grid, internet, or telecommunications network, as well as any failure, delay, or unavailability in the delivery or receipt of push notifications, SMS messages, or emails attributable to telecommunications operators, messaging service providers, or third-party email platforms.
- Improper integration, configuration, or use of the Software contrary to the specifications contained in the technical Documentation or instructions provided by IRONCHIP to the Client.
- Acts or omissions attributable to the Client's personnel, clients, suppliers, or any third party unrelated to IRONCHIP.
- Exploited vulnerabilities or security incidents or data breaches resulting from the Client's omission or delay in implementing patches, updates, or new versions of the Software that have been notified and made available by IRONCHIP for the purpose of mitigating risks or correcting potential security flaws.

7.7. Neither Party shall be liable for any failure or delay in fulfilling their obligations if such failure or delay is due to force majeure. Force majeure shall include all events that could not have been foreseen or prevented with reasonable measures, as well as changes in applicable law that may affect the scope or provision of the contracted services and could not have been foreseen.

7.8. **Third-Party Services:** The Software may interoperate, integrate, or partially or fully depend on services provided by third parties, such as electronic communications providers, messaging services (including SMS via platforms like AWS SNS), push notifications, email services, cloud services, external authentication systems, SCIM/LDAP/Active Directory integrations, third-party APIs, as well as any infrastructure, tool, or technological component not directly provided by IRONCHIP (hereinafter, "Third-Party Services"). Third-Party Services are provided "AS IS" and "AS AVAILABLE," and are subject exclusively to the terms, conditions, and policies of such third parties. IRONCHIP does not guarantee the availability, continuity, compatibility, security, performance, maintenance, support, or suitability of the Third-Party Services, and shall not be liable for errors, interruptions, data loss, delivery failures, delays, vulnerabilities, or issues directly or indirectly attributable to Third-Party Services. The Client acknowledges that: (i) the proper functioning of the Software may depend on the availability and adequate provision of Third-Party Services; (ii) IRONCHIP does not control or manage such services; and (iii) any disruption or malfunction of these Third-Party Services shall not be deemed a breach of the Agreement by IRONCHIP. In the event that a Third-Party Service is discontinued, modified, becomes unavailable, or affects the operation of the Software, IRONCHIP will make reasonable efforts to mitigate the effects, but shall not be obligated to provide replacements, alternatives, refunds, compensation, or indemnification, nor shall it assume any liability for such changes.

8.- INDEMNIFICATION

8.1 IRONCHIP shall defend the Client against any third-party claim alleging that the Software, when used in accordance with these Terms and the applicable Documentation, infringes such third party's intellectual property rights. IRONCHIP shall bear the damages and legal costs either legally agreed upon or finally awarded to the Client in connection with such claim.

8.2 However, the above obligation shall not apply if the alleged infringement results from any of the following circumstances:

(i) the use of the Software together with products, services, data, components, or content not provided by IRONCHIP;
(ii) any modification, alteration, or adaptation of the Software made by the Client or by third parties at the request or for the benefit of the Client;
(iii) the use of a previous version of the Software when IRONCHIP has made available to the Client a modified or updated version whose use would have avoided the infringement;
(iv) the use of the Software in combination with third-party systems, architectures, infrastructures, components, integrations, APIs, cloud environments, configurations, or services not approved by IRONCHIP, or that alter, interfere with, or affect the intended

operation of the Software;
(v) developments, requirements, instructions, designs, configurations, or specifications provided by the Client or by its consultants, technology providers, integrators, or third parties acting on its behalf;
(vi) the use of the Software outside the scope of the License, in contravention of these Terms and Conditions or the Documentation.

8.3 In the event that an infringement claim is likely or occurs, IRONCHIP may, at its sole discretion and as the sole remedy, take any of the following actions:

(a) modify the Software to make it non-infringing while maintaining substantially equivalent functionality;
(b) replace the Software with a non-infringing version with equivalent functionality;
(c) obtain for the Client a license or authorization allowing continued use of the Software; or
(d) if none of the foregoing options is reasonably feasible, terminate the Subscription Agreement with respect to the affected component and refund the Client a proportional amount of the fees already paid for the unused period.

The measures set out in this clause 8.3 (including, as applicable, defense, replacement, modification, or termination with proportional refund) shall constitute the Client's sole and exclusive remedy against IRONCHIP for any third-party claim based on alleged infringement of intellectual property rights.

8.4 The Client shall defend, indemnify, and hold harmless IRONCHIP, as well as its directors, employees, affiliates, and subcontractors, from and against any damage, loss, penalty, liability, claim, or expense (including reasonable attorney's fees) arising from or related to: (i) any breach by the Client or its Authorized Users of the Software use restrictions established in these Terms, including, but not limited to, clauses 2.3, 2.5 (Acceptable Use Policy), and 3; (ii) the use of the Software by the Client or its Authorized Users in contravention of these Terms and Conditions, the Subscription Agreement, the Documentation, or applicable law; (iii) any claim arising from the accuracy, quality, lawfulness, completeness, or adequacy of the data, information, or content provided, uploaded, or managed by the Client or its Authorized Users through the Software; (iv) access to or use of the Software by affiliates, providers, consultants, subcontractors, or third parties to whom the Client has directly or indirectly permitted access or use of the Software, pursuant to clause 4.2; (v) any claim arising from the use of the Software in combination with systems, configurations, integrations, APIs, architectures, infrastructures, or Third-Party Services not approved or not provided by IRONCHIP; (vi) any use of the Software that results in risk to the security, integrity, or availability of the service, including malicious, negligent, or otherwise unacceptable actions under the Acceptable Use Policy.

8.5 The Client's indemnification obligation under clause 8.4 shall be in addition to, and shall not limit, the Client's other contractual obligations, including those related to payment of fees, correction of usage excesses under clause 2.3 (Usage Restrictions and License Usage Verification), and compliance with applicable regulations.

9 SECURITY OF THE SOLUTION AND CUSTOMER DATA

9.1. IRONCHIP shall implement and maintain appropriate technical and organizational security measures consistent with industry standards to protect the Licensed Solution, the infrastructure through which the service is provided, as well as the Customer's Confidential Information and data (including personal data), against threats to confidentiality, integrity, and availability. IRONCHIP's Information Security Management System (ISMS) is certified under ISO 27001 (Information Security) and ISO 27701 (Privacy Management), and the platform complies with the National Security Framework (ENS) at its High level, providing a security framework aligned with recognized standards and best practices, which the Customer may use as part of its compliance strategy with NIS2, DORA, and other sector-specific regulations. However, this shall not constitute a guarantee of compliance by IRONCHIP with the Customer's specific legal obligations.

9.2. Such measures shall include, among others and as applicable:

- Logical and physical access controls.
- Robust authentication mechanisms (relevant for an identity product).
- Data encryption at rest and in transit.
- Capabilities to ensure system and service resilience and recovery (backups).
- Vulnerability detection and mitigation programs.

9.3. IRONCHIP shall maintain a security incident management procedure and shall notify the Customer without undue delay of any incident affecting the Customer's data or systems, in accordance with the specific notification obligations set forth in Clause 6 (Personal Data Protection).

9.4. The Customer is solely responsible for securely configuring and using the Software, including proper management of permissions, access credentials, and the configuration of security policies within the platform, in accordance with the Documentation.

10.- MAINTENANCE AND SUPPORT

10.1. The acquisition of License(s) by the Customer includes Standard Support, which shall be provided under the following conditions:

10.2. **Support Levels:** Standard Support is divided into three levels based on the complexity of the query or the issue with the service:

- **Level 1: Basic Support (First-Level Support)**
    - **Responsible party:** Trained Customer, trained Distributor, or IRONCHIP.
    - **Description:** This level is the Customer's first point of contact and handles basic queries, common issues, and information requests.

- **Main functions:** Receiving and logging incidents, initial diagnosis, resolving simple problems such as basic configuration or FAQs, and escalating unresolved incidents to Level 2.
- **Tools:** Knowledge bases, user guides, FAQs, and troubleshooting scripts.

- **Level 2: Specialized Technical Support (Second-Level Support)**

  - **Responsible party:** Trained Distributor or IRONCHIP.
  - **Description:** This level focuses on solving more complex technical issues that cannot be resolved at Level 1. It requires personnel with advanced knowledge of the products and services offered.
  - **Main functions:** Detailed technical analysis, resolution of issues related to implementation, configuration, or technical behavior of the products, and escalation of critical or structural cases to Level 3.
  - **Tools:** Diagnostic tools, access to advanced technical documentation, and remote support.

- **Level 3: Expert and Manufacturer Support (Third-Level Support)**

  - **Responsible party:** IRONCHIP.
  - **Description:** This is the highest level of support, responsible for resolving critical problems, software bugs, security vulnerabilities, or failures that require direct manufacturer intervention.
  - **Main functions:** Investigation of critical failures, resolution of issues that cannot be addressed by the Distributor, development of necessary patches or updates, and assistance in the detection and mitigation of cybersecurity vulnerabilities.
  - **Tools:** Access to source code (if applicable), development tools, testing labs, and specialized engineering teams.

10.3. **Incident Categorization and Response Times:** Support varies according to the criticality level of the incident, as detailed in the following table. IRONCHIP reserves the right to adjust the priority of incidents after conducting an initial analysis of the situation.

Category	Description	Impact	Support Availability	Response Time
1 –Low Priority	General questions about the product and custom requests that do not affect the service's operation or performance. Examples: Informational inquiries, documentation requests, non-urgent customizations.	No operational impact.	Monday to Friday, 8:00 to 17:00 (8x5), via email.	Maximum 7 days.

2 – Medium	Issues that do not significantly affect the service or have minimal customer impact. Examples: General technical inquiries, minor UI errors, configuration issues without critical impact.	Affects less than 10% of authentications or does not interrupt the service.	Monday to Friday, 8:00 to 17:00 (8x5), via email.	Maximum 72 hours.
3 – High	Issues that partially affect the service but do not prevent its overall operation. Examples: Intermittent failures, issues affecting between 10% and 75% of authentications, incidents requiring temporary solutions.	Affects between 10% and 75% of authentications.	Monday to Friday, 8:00 to 17:00 (8x5), via email.	Maximum 24 hours.
4 – Critical	Critical issues causing total service loss or severely affecting more than 50% of authentications. Examples: Total service outage, critical security vulnerabilities, massive authentication process failures.	Affects more than 50% of authentications or completely interrupts the service.	24 hours a day, 7 days a week (24/7), via dedicated emergency phone number.	Maximum 4 hours.

10.4. **Availability (SLA):** The IRONCHIP Management Panel will be available 99.5% of the time. The availability indicated in clause 10.4 constitutes a service level objective ("SLA") for guidance purposes only and does not represent a strict contractual guarantee or an obligation of result on the part of IRONCHIP. Any failure to meet the SLA shall not, under any circumstances, entitle the Client to automatic compensation, penalty, refund, service credit, or early termination. Any impact resulting from availability levels below the stated objective shall be managed exclusively through the support measures set out in this section 10 and within the liability limits established in clause 7.

10.5. **Communication Channels:** Incidents and requests shall be handled via email at support@ironchip.com. For critical incidents (Category 4), a dedicated 24/7 phone number will be made available, which will be communicated to the Client.

11.- TERM AND TERMINATION

11.1. **Term:** These General Terms and Conditions shall enter into force on the date of signature of the Subscription Agreement and shall remain in effect for as long as there is an active Subscription Agreement or until its termination in accordance with this clause.

11.2. If the Client requires early termination of the Subscription for any reason before the full Subscription period has ended, such termination shall not entail any refund or reimbursement by IRONCHIP to the Client for amounts previously paid, nor shall it release the Client from payment of any remaining Subscription years pending invoicing and/or payment as of the early termination date with respect to the full Subscription period.

11.3. A material breach by either Party of the obligations set forth in these Terms and Conditions or in the Subscription Agreement may lead to termination of the Agreement by the non-breaching party, subject to prior written notice to the breaching party granting a reasonable period to remedy the breach.

11.4. Upon termination of the License, for any reason, the Client must immediately cease using the Software and, if applicable, uninstall it from all systems and devices. The clauses relating to Intellectual Property, Confidentiality, Limitation of Liability, Data Protection, Applicable Law, and Jurisdiction shall survive termination.

12.- GENERAL PROVISIONS

12.1. **Independence of the Parties:** The Parties are independent legal entities, and this agreement does not create any partnership, subordination, agency, or employment relationship between them.

12.2. **Entire Agreement:** These Terms and Conditions, together with the Subscription Agreement, constitute the entire agreement between the Parties with respect to the subject matter hereof and supersede any prior agreements or understandings, whether verbal or written. In the event of any contradiction, inconsistency, or lack of regulation regarding any matter between these Terms and the Subscription Agreement, the conditions set forth in the Subscription Agreement shall prevail in all cases.

12.3. **Amendments:** These Terms and Conditions constitute an adhesion contract and are not individually negotiable. IRONCHIP may update or amend them at any time for technical, operational, legal, regulatory, or service-related reasons. Any modification will be communicated to the Client with reasonable advance notice (at least 30 days) via email or through the Software itself. Continued use of the Software after the effective date of the modifications shall imply full acceptance of the new Terms and Conditions.
Modifications to the Subscription Agreement, including financial terms, scope, duration, or any particular condition, shall always require the written agreement of both Parties and may not be unilaterally made by IRONCHIP.
If the Client does not wish to accept the modifications to the General Terms and Conditions, they may terminate the Subscription effective as of the date the new terms come into force, without the right to reimbursement of any amounts already paid, unless otherwise provided by applicable law.

12.4. **Assignment:** The assignment of the License or of the rights and obligations arising from this agreement by one of the Parties to a third party shall require the prior express written consent of the other Party to be valid and effective.

12.5. **Export Control and Sanctions:** The Client represents and warrants that neither they nor their Authorized Users:

(i) are listed on any international sanctions or restrictions lists issued by the European Union, the United Nations, the United Kingdom, or the United States (including, but not limited to, OFAC, BIS, or equivalent lists);
(ii) are established, operate, or use the Software from countries or territories subject to applicable sanctions or embargoes;
(iii) will use the Software directly or indirectly for purposes prohibited by European or international regulations on export control, anti-terrorism, illicit financing, or economic sanctions.
The Client shall be responsible for ensuring compliance with such regulations and shall take the necessary measures to prevent access to the Software from locations or by persons not authorized under applicable law. IRONCHIP may immediately suspend access to the Software and/or terminate the Subscription Agreement without prior notice if it reasonably believes that the Client or an Authorized User is in breach of this clause, without any right to reimbursement or compensation.

12.6. **Severability**: The invalidity of any provision of this agreement shall not affect the validity or enforceability of the remaining valid provisions.

12.7. **Notices**: Any formal notice required to be made under or in connection with the Agreement shall be made in writing and sent to the registered office of each of the Parties by any means that provides proof of receipt by the recipient. In any case, communications sent by email between the Parties shall be fully valid and effective when sent through the contact persons and addresses designated for that purpose by each Party.

Contact details for notifications to IRONCHIP:

- **Email:**
  - Billing: administracion@ironchip.com
  - Support: support@ironchip.com
  - Security: security@ironchip.com
  - Data Protection: privacy@ironchip.com
  - Data Protection Officer: dpo@ironchip.com

- **Regular postal mail:**
  - To the attention of: IRONCHIP TELCO S.L. - Administration
  - Postal address: Calle Beurko Viejo, 17 – 48902 Baracaldo, Vizcaya (Spain)

Any changes to the notification addresses must be communicated to the other Party in accordance with the provisions of this clause. Until a Party receives notice of such changes, any notifications made pursuant to this clause and based on the original details shall be deemed to have been duly made.

12.8. **References**: The Client authorizes IRONCHIP to use its logo, trade name, and reference as a Client on IRONCHIP's website and in presentations and communications, without disclosing any confidential information related to the Client or the Subscription Agreement.

13.- APPLICABLE LAW AND JURISDICTION

13.1. This document and the governing Software License are subject to Spanish law.
13.2. The Parties shall endeavor to resolve in good faith any dispute or controversy that may arise in connection with or as a result of the Software License. If the dispute cannot be resolved amicably through negotiation, the Parties agree to submit any potential disputes to the exclusive jurisdiction of the courts and tribunals of Bilbao (Spain), expressly waiving any other jurisdiction that might otherwise apply.

Date of Last Update: January 2026