SECURITY APPENDIX

1. SUBJECT MATTER OF THE AGREEMENT: This Security Appendix sets out the measures to protect the information shared between BELLTECH and its providers. This applies to all of BELLTECH's providers and the personnel involved in relationships with providers.

2. OWNERSHIP OF INFORMATION:

1. BELLTECH retains sole ownership of all information shared with THE PROVIDER, including designs, trademarks, and intellectual property rights. This includes studies, reports and data generated during the execution of the contract.

2. THE PROVIDER may not reproduce or trade the information, unless otherwise provided.

3. THE PROVIDER may process certain information for the service but must ensure its security.

4. THE PROVIDER must keep records of the operations related to the information provided by BELLTECH for at least five years.

3. RESTRICTIONS ON THE SOFTWARE USED:

1. In the event that THE PROVIDER has access to BELLTECH's software or that of its contractors, THE PROVIDER shall not reproduce, distribute or trade BELLTECH's software, nor shall it permit unauthorized access to it. THE PROVIDER agrees to use the software only according to BELLTECH's instructions and not to modify it or reverse engineer it. In the event of infringement of intellectual property rights, the PROVIDER shall compensate BELLTECH for any damages.

2. THE PROVIDER shall use safe software to protect BELLTECH's information and shall allow security testing by BELLTECH. If the software fails to meet the security requirements, BELLTECH reserves the right to reject its use.

3. If the PROVIDER uses free software or cloud services, they must ensure proper support and the integration with BELLTECH's authentication systems.

4. PROCEDURES IN CASE OF ALTERATION OR MANIPULATION OF DEVICES OR INFORMATION

1. In the event that during the execution of this contract, evidence arises of alteration or manipulation of equipment or information that is the property of BELLTECH, used in the execution of the contract or purchase order, THE PROVIDER shall inform said situation to the person in charge of THE CONTRACTING PARTY, mentioned in this contract, as well as to the email address sig@belltech.la, providing evidence demonstrating such eventuality and the actions taken to mitigate any damage to BELLTECH.

2. When manipulation or alteration of BELLTECH's Software, Hardware, or information is detected, THE PROVIDER shall immediately cease its use and restrict access to contractors and officials.

3. THE PROVIDER shall have the means and procedures to collect, store, and provide the information required by BELLTECH, maintaining the chain of custody according to legal regulations.

4. THE PROVIDER shall be responsible to BELLTECH, third parties, and authorities for the proper handling of information.

5. BELLTECH may collect information if deemed necessary.

6. THE PROVIDER shall provide application and data records as per the requirement of forensic computing or security analysis.

5. PROCEDURES FOR DELIVERY AND DESTRUCTION OF INFORMATION BY THE PROVIDER-

1. Delivery of Physical Information:

a. The delivery of physical documents from BELLTECH shall be conducted with evidence of delivery, traceability in shipping and receiving systems, or through technological means.

b. Depending on the service, additional delivery procedures may be required, as informed by BELLTECH.

2. Delivery of Electronic Information:

a. THE PROVIDER shall ensure the security of transmitted electronic information, preventing unauthorized access or modification.

b. Control and security systems must be implemented to certify the integrity and restriction of access to the information.

3. Destruction or Return of Information:

a. Upon completion of services, THE PROVIDER must return or destroy the information as instructed by BELLTECH.

b. The return or destruction shall be completed within 30 business days, subject to BELLTECH's authorization.

c. If authorization is not granted, THE PROVIDER must request instructions within the following 60 business days.

d. THE PROVIDER shall ensure confidentiality during the destruction process and shall enter into confidentiality agreements with those responsible for destroying the information.

Information stored in the cloud shall be securely erased before delivering the resources, and storage and retention requirements shall be defined with BELLTECH.

6. CONTINUITY OF THE SERVICES PROVIDED

1. THE PROVIDER must have a continuity plan to handle internal and external incidents that may disrupt services.

2. The plan must be documented and reviewed every 6 months to ensure its effectiveness against various scenarios.

3. Relevant collaborators of the provider shall be informed about these procedures.

4. BELLTECH has the right to verify the effectiveness of the plan by requesting documentation and conducting planned visits.

SECURITY APPENDIX

5. The Business Continuity Plan includes policies, strategies, procedures, and tasks to maintain service continuity.

7. INFORMATION SECURITY STANDARDS: THE PROVIDER shall comply with BELLTECH's security policies established in the “INFORMATION SECURITY POLICIES ANNEX.” Additionally, the PROVIDER shall provide services following industry best practices and complying with established standards to ensure information security. BELLTECH shall have the right to request reports on the standards applied by THE PROVIDER.

8. SECURITY OF INFORMATION: To ensure information security, THE PROVIDER must:

1. Implement an information security and cybersecurity program certified by an external auditor, in accordance with international standards such as ISO 27001 or other applicable standards, including: **I.** Annual security training. **II.** Advanced threat protection. **III.** Incident management and response. **IV.** Vulnerability testing. **V.** Processes for preventing information leakage. **VI.** Mechanisms for controlling access to information.

2. Notify BELLTECH of any modifications to security procedures.

9. CLOUD SECURITY (Applies only to cloud services contract)

1. THE PROVIDER must comply with the standard defined by BELLTECH for cloud services, ensuring availability and modification of information, as well as security incident management. Information must be hosted in countries with data protection laws.

2. Both parties must have defined responsible parties for information security. BELLTECH may request information at any time, and THE PROVIDER must respond to these requests within the agreed-upon deadlines.

3. THE PROVIDER must follow the cloud security framework, including standards such as ISO/IEC 27017, ISO 27018, SSAE 16 SOC1, SOC2, SOC3, CSA STAR, and PCI DSS if applicable. If these certifications are not in place at the time of contract signing, THE PROVIDER has a maximum of twelve months to establish them, initiating the process within sixty days. Any exceptions must be validated with the Information Security departments.

10. INFORMATION SECURITY CHANGE MANAGEMENT: THE PROVIDER must inform BELLTECH of any changes that may affect information security in the provision of the service.

11. SECURITY OF INFORMATION FILES AND DATABASES: To ensure the security of BELLTECH’s files and databases, THE PROVIDER must:

1. Store BELLTECH’s confidential information in encrypted format.

2. Place servers and data repositories in physically secure areas.

3. Restrict physical and logical access as per business need.

4. Protect access with a combination of user identification and password.

5. Record all access activity and transactions.

6. Handle backup copies with strict security controls.

7. Use security analysis tools to review database configurations.

8. Periodically review all security controls to ensure their effectiveness.

12. BACKUP AND RECOVERY: To meet BELLTECH’s requirements and industry best practices for backup and recovery, THE PROVIDER must:

1. Implement appropriate backup measures, including secure off-site storage of files.

2. Facilitate the resumption of critical applications and business activities after emergencies.

3. Maintain a documented disaster recovery plan and test it.