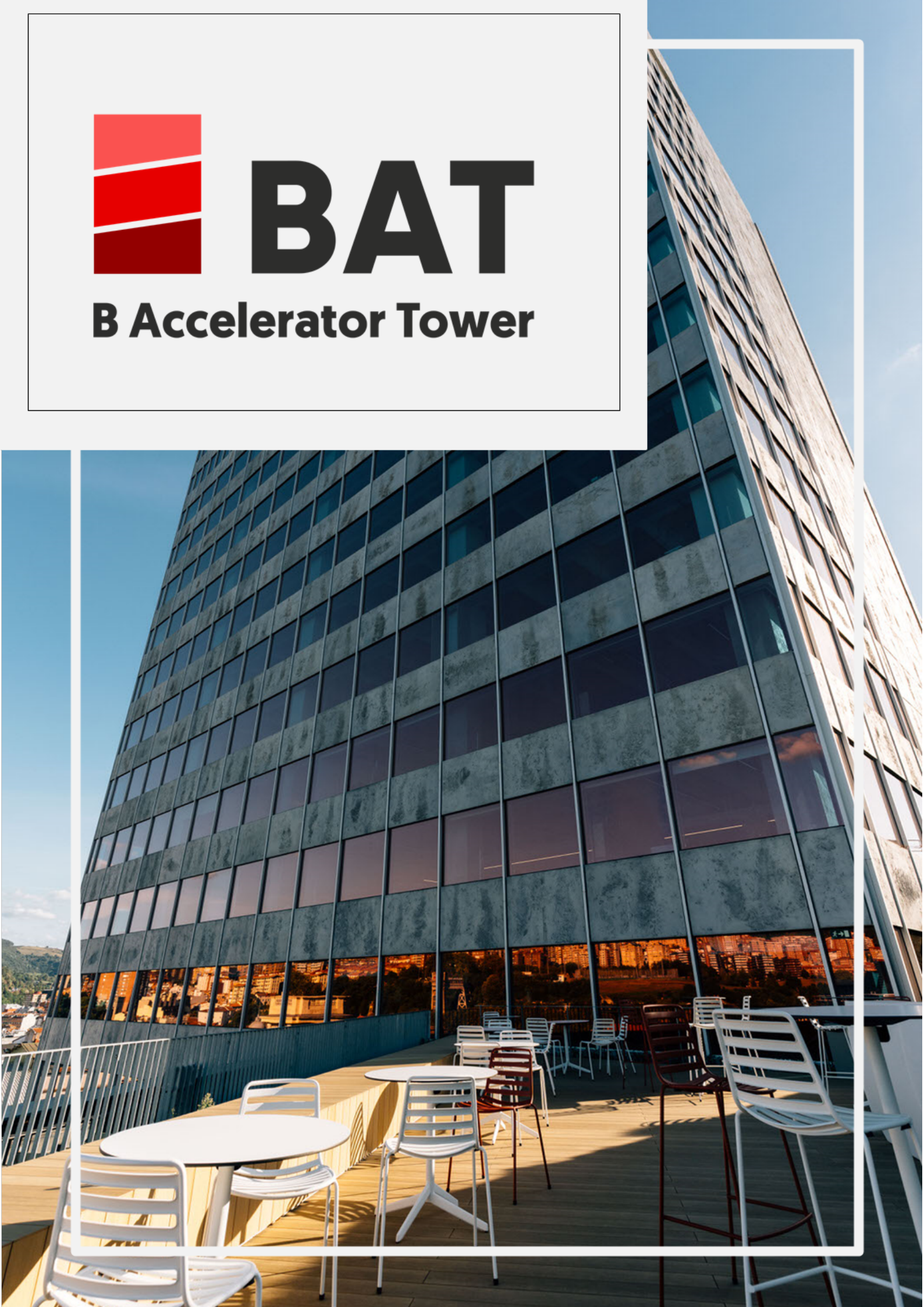
BAT

B Accelerator Tower



Iberdrola Open Innovation Challenge

Automatic birdlife detection and deterrence systems with automatic shutdown

1. Exposition

Iberdrola is a global energy group active in electricity networks, renewable energy, storage and energy retail. Its strategy is focused on driving a more sustainable energy model, supported by innovation, electrification and the development of infrastructure that contributes to the decarbonisation of the economy.

PERSEO is Iberdrola's open innovation and start-up support programme, created to bring the group closer to technologies and business models with strategic potential for the future of the energy sector. Through technological challenges, pilots, proofs of concept, partnerships and investments, PERSEO facilitates collaboration between Iberdrola and emerging companies that provide technological solutions acting as a lever for transformation within the Iberdrola Group.

BAT B Accelerator Tower is one of the best-connected entrepreneurship and innovation ecosystems in the world, offering a unique collaborative, entrepreneurial and innovation space located in Bilbao, Bizkaia. BAT is the spearhead of a project aimed at placing Bizkaia on the international entrepreneurship map and strengthening the competitiveness of its economy by fostering collaboration between major local corporations and leading technology companies — including start-ups, scale-ups and innovative SMEs — as well as innovation hubs and investors from around the world.

2. Background

Iberdrola has close to 7,000 MW of installed wind power capacity in Spain, in a context where sustainability and biodiversity protection have become key priorities for the development and operation of renewable energy facilities. Within this framework, and in line with increasingly demanding requirements set out in Environmental Impact Statements for both new projects and assets already in operation, the company has been incorporating birdlife detection systems and automatic wind turbine shutdown mechanisms when the presence of birds is identified in the vicinity of the turbines.

However, the experience gained to date shows that the effectiveness of the available solutions may vary significantly across technologies. This, together with the high cost of the equipment and its maintenance requirements, limits the feasibility of large-scale deployment. The market currently relies mainly on solutions based on stereoscopic camera configurations or radar-camera combinations, while other alternatives, such as deterrence systems, still show a limited degree of development and validation, with an offering that remains insufficiently mature to robustly address the sector's operational needs.

3. Executive Summary of the Challenge

Through this challenge, Iberdrola seeks to identify technological solutions capable of improving birdlife protection in wind power environments, combining operational effectiveness, economic viability and ease of integration into its facilities. The objective is to move towards autonomous and scalable systems that can detect birds in the vicinity of wind turbines, determine their position and trajectory in real time and, where there is a risk of collision, trigger the controlled shutdown order of the wind turbine through the wind farm's UCC (Control Unit) with sufficient advance notice.

Alongside this first line of work, the challenge also aims to identify deterrence systems capable of modifying birds' risk trajectories without the need to stop the wind turbines, always from an approach that is respectful of biodiversity and compatible with wind farm operations.

In this regard, proposals focused on only one of the areas described will be accepted, as well as integrated solutions combining detection and deterrence within a single technological approach.

4. Challenge Description

For the assessment of proposals, a set of prior requirements has been established that must be met. These requirements are the result of the experience gained in recent years working with birdlife systems, as well as the operational needs of the wind power business

- The system must be low-cost compared with existing market solutions, and annual maintenance must also be cost-effective.
- It must be 3D, positioning birds in space at all times.
- The system must be easily calibratable and configurable in the field.
- It must include an on-site viewer with the ability to display trajectories.
- It must include a private-use web application to store different bird trajectories, photographs and videos, and to enable both searches and potential forensic analysis in the event of bird collisions.
- In the case of camera-based systems, it may include species recognition based on the images or videos obtained. Recognition must be carried out at species level — for example, red kite — and not at genus level — for example, kite.
- The systems must be capable of detecting birds at a distance from the wind turbines that allows their controlled shutdown, which shall under no circumstances be performed using the emergency brake.
- The birds to be detected will range from a wingspan of approximately 0.60 metres to 2.50 metres. If the system is not capable of detecting birds with a wingspan of 0.60 metres, the detection limits must be specified.
- The equipment must be designed for permanent outdoor installation.
- Connection to Iberdrola's facilities must be included. All signals must comply with Iberdrola's cybersecurity protocols.
- Any shutdown shall be carried out through Iberdrola's UCC.

- Preferably, the equipment shall be installed on existing infrastructure — for example, on wind turbine towers, and never welded to them. External poles or towers shall be avoided as far as possible, as they require longer cable routing and create new impacts for landowners.
- The proposed deterrence systems must be respectful of both birdlife and the local conditions of the wind farm installation sites and must comply with applicable legislation.
- The system must be supported by parallel calibration, to be defined by the bidder, enabling the determination of the bird detection rate at different distances, the effectiveness of the deterrence system and, where applicable, the accuracy rate for species detection.

The proposals to be considered must demonstrate the following key attributes:

- Maturity and reliability of the solution.
- Optimisation of investment and operating costs.
- Implementation costs and required personnel.
- Ease of implementation and use, with minimal training required.
- Minimisation of the number of birdlife-related shutdowns.
- Respect for birdlife.
- Compliance with health, safety and environmental standards (HSE).

5. Challenge Objectives & Types of candidates

The main objective is to identify innovative solutions within the field described above and to promote collaborative projects between start-ups/technology companies and the organisation promoting the challenge.

Any entrepreneur, start-up, SME or technology company with a proposal that could contribute to the partial or full resolution of the challenge may participate. Organisations interested in offering their solution to the challenge do not need to be located in the territory of Bizkaia or to be an active part of the BAT B Accelerator Tower business community.

The challenge is primarily aimed at:

- Legally incorporated companies, with no restriction regarding the date of incorporation.
- Innovative companies offering solutions based on technological developments and with the capacity to undertake R&D projects to address the needs described.
- Companies with a product already on the market or with technological developments equivalent to TRL 7 or above, which can be tested in real-life environments.
- Companies with the capabilities and solvency required to collaborate with large corporations.
- Companies with the capacity to develop the pilot in Spain.
- A single start-up, SME or organisation may participate with only one project, either individually or jointly with third parties.

6. Main Phases and Key Milestones

PHASE	DATE	DESCRIPTION
Application period	From 25/06/2026 to 21/08/2026	Candidates' acceptance period
Evaluation of candidates	From 31/08/2026 to 11/09/2026	Internal evaluation of candidates
Selected startups Announcement	14/09/2026	Notification by e-mail
B2B Meetings with Iberdrola	Starting 15/09/2026	Business Meetings

7. Application Process

The application period will be open from 25/06/2026 to 21/08/2026 through the BAT B Accelerator Tower website, under the "Open Opportunities" section. Organisations interested in participating in this initiative must complete the corresponding application form, attaching to their application any information required or considered relevant.

- Applications must be completed in Spanish or English.
- Only one application per company will be evaluated; if more than one application is submitted, the latest application received will be assessed.
- Once the application has been received, an automatic confirmation of receipt will be sent.
- The application form shall contain the following information:
    - General company information and contact details.
    - Proposed solution and development status.
    - Innovation elements — product, process, marketing and organisation — or R&D results related to the proposed solution.
    - Technologies associated with the proposed solution, where applicable.
    - Team that will participate in the development of the solution.
    - Risks and benefits.
    - Partners.
    - Cost and Timeline.
    - Confirmation that the solution complies with Iberdrola's cybersecurity specifications

8. Selection Process

In order to select the best projects, an evaluation team will be established comprising representatives from Iberdrola and BAT, who will be responsible for carrying out the selection process.

Once the application submission period has ended, BAT will conduct an initial quality review of the applications received, excluding any applications that have not properly completed the required information. The designated Iberdrola representatives will analyse the applications submitted and assess each of them from a technical perspective, with a view to drawing up a shortlist of projects.

The evaluation team will assess the following aspects of each of the finalist proposals:

- Innovation: the degree of innovation of the proposed solution will be assessed.
- Project maturity: the level of development of the proposed solution.
- Project team: the team of the participating organisation(s) will be assessed, including their experience, commitment, market knowledge, contacts, etc.
- Timeline: the timeframe within which the solution could become operational in the market.
- Feasibility: the feasibility of the project, as well as the cost of the solution and its maintenance in a real-life environment.
- Project scope: the extent to which the proposed solution responds to the challenge and how it addresses the issue identified

Compliance with the above requirements must be evidenced at the time of submission of the application through the form designed for this purpose, to which the relevant additional documentation may be attached, including any necessary annexes, to verify compliance with the required criteria.

9. Relationship Between the Challenge-Promoting Company and the Candidate Companies

Iberdrola's objective in this process is to identify companies with which it can launch a pilot project within a maximum period of three months following the announcement of the winner. The proposed pilot will enable the selected company to collaborate with Iberdrola at a wind farm located in Spain, with the possibility of a follow-up and scaling contract or long-term collaboration if the pilot is successful.

Throughout the process, the candidate start-up/technology company undertakes to allocate the necessary human and material resources to carry out the proposed activities, including individuals empowered to make decisions regarding technological and business development, as well as to respond to official communications.

The representative must be over 18 years of age, hold a C-level position within the company, and be able to communicate fluently in English or Spanish at all levels, acting as the company's representative.

This person must meet the legal requirements necessary to reside and remain in Spain. Likewise, the candidate must be up to date with all tax, fiscal and social security obligations.
All notifications relating to the development of the challenge will be sent by email directly to the representative. Candidate companies must provide a telephone number to handle any communications that may require it.

10. Aceptación de Términos y Condiciones Acceptance of Terms and Conditions

The following terms and conditions are intended to establish the rules for participation in this process. Participation in this call entails the full and unconditional acceptance of these Terms and Conditions without exception.

11. Política de confidencialidad y protección de datos

Participation in this call is voluntary. The content of the applications submitted through the application form, as well as all documentation and information of any kind provided, shall be confidential and private, and shall be treated as such by the company promoting the challenge.

Candidate companies accept, as a general rule, the use by the company promoting the challenge of the basic project data during the evaluation and selection processes described in these Terms and Conditions.

Participation in the challenge does not grant any rights over the intellectual property of the applications merely by taking part in this call. Candidate companies must ensure that the work and content voluntarily provided through the form linked to the challenge, including summaries or presentations, do not infringe third-party rights and that they hold all necessary authorisations to participate in this challenge.

Furthermore, such content must not be offensive or degrading, incite violence or racism, or violate the fundamental rights or public freedoms recognised under applicable legislation, including laws on the protection of children and young people.

Nor must it constitute or involve intrusions into the personal or family privacy of individuals, infringe the right to honour or the confidentiality of third-party communications, or breach any applicable regulations. In addition, the projects submitted must ensure the non-sexist use of language and images.

Finally, each participating start-up/technology company authorises the company promoting the challenge to use its name and image in dissemination materials related to the challenge, including those published on the Internet, without receiving any compensation in return.

12. Intellectual Property Rights

The candidate company guarantees that it holds the appropriate exploitation rights over the products, services, patents, utility models and any other content included in its application. Participating companies shall hold the challenge-promoting company harmless from any claim arising from the infringement of third-party rights, including infringements of intellectual and industrial property rights.

The participating candidate shall not be required to grant any intellectual or industrial property rights to the challenge-promoting company, except for the exceptions set out in these Terms and Conditions. If the candidate company and the challenge-promoting company agree to carry out collaborative work to jointly design or co-create solutions, both parties shall establish, in a separate private document, the terms relating to intellectual and industrial property and to the commercialisation of the resulting solution.

13. Applicant Declaration

By submitting their application, candidate companies declare and warrant to the challenge-promoting company that:

- The applications submitted are original works of their authors and/or that they freely hold the rights to use any ideas, images or other elements included in their submission.
- They have obtained the consent of all third parties whose personal data have been included in their application.
- The information provided does not contain confidential information belonging to themselves or to third parties, nor any trade secrets or, where applicable, that they hold the necessary authorisations and licences allowing its disclosure within the framework of this call.
- They have full legal capacity and authority to participate in the call, and that such participation does not breach any regulations of any kind.
- They shall assume any taxes arising from participation in this call, as well as from the potential receipt of any financial contributions provided for under the challenge.
- The challenge-promoting company shall not be liable for any damages, losses, costs and/or claims that candidates may suffer or incur as a result of submitting their applications.
- The proposed solution meets Iberdrola's cybersecurity requirements (see Annex 1).

14. Contact and Inquiry Resolution

For any questions or clarifications, you may contact the BAT B Accelerator Tower management team at the following email address: info@bacceleratortower.com

Official Website: [BAT B Accelerator Tower website].

Annex 1 - Cybersecurity

The aim shall be to ensure the protection of the technological infrastructure, the availability of generation systems, the integrity and confidentiality of data, as well as regulatory compliance in cybersecurity matters in accordance with ISO 27001, IEC 62443 and the NIS2 Directive.

The Contractor shall ensure that all system communications are carried out through secure protocols, avoiding the use of unencrypted protocols.

All data in transit shall be encrypted using TLS 1.2 or higher, while data at rest shall be encrypted using AES-256.

The Contractor undertakes to ensure that all software applications developed and implemented within the service comply with secure development principles and have undergone DAST and SAST security analysis before being put into production.

The architecture shall include appropriate network segmentation, with the implementation of perimeter firewalls to ensure the isolation of the different system components, including data processing and storage infrastructure, as well as its integration with control systems.

The security infrastructure shall include next-generation firewalls with IDS/IPS capabilities, approved by the CORE Communications and business Cybersecurity managers, such as Palo Alto or other equivalent solutions enabling real-time threat detection and blocking.

The Contractor shall establish identity and access management policies applying the principle of least privilege, ensuring that each user has only the permissions strictly necessary for their role.

All remote connections for the administration of systems or equipment providing services to the Client or interacting with its infrastructure shall be carried out through mechanisms incorporating multi-factor authentication.

Remote connections shall be made exclusively through virtual private networks (VPNs) that comply with the security standards defined by the organisation. This requirement applies both to occasional access and to continuous monitoring connections.

All devices intended for network access, including, among others, 4G/5G routers, shall be the exclusive property of the Client, who shall at all times retain full control and governance, administration and configuration capabilities over them. The use of equipment not under such direct control is prohibited.

The exposure of routers with public IP addresses is prohibited, and traffic filtering mechanisms must be implemented to restrict unauthorised access.

The Contractor shall ensure that all devices used in the service, including routers and servers, have appropriate protection measures in place.

Physical security of the devices shall be properly managed through locked cabinets or similar protection elements, in order to restrict access to the equipment to authorised personnel only.

It shall be ensured that all servers and communication devices used to provide the service have hardening configurations in place, in accordance with industry best practices and standards such as CIS.

A preventive maintenance plan shall be implemented, covering the periodic updating of firmware and software, as well as verification of the operational status of the devices in service.

The Contractor may view and consume the data generated by the system once such data have been stored in a secure infrastructure owned by the Client, either in previously authorised cloud environments — such as AWS, GitHub or the Client's private platforms — or in local facilities under strict control.

A data classification and retention policy shall be implemented, taking into account the confidentiality of the information generated by the system, particularly records whose public exposure could have an impact on the Client. In this regard, the need for data anonymisation prior to processing or storage shall be assessed.

The processing infrastructure shall incorporate monitoring mechanisms to detect alterations in the information captured by the system — threshold parameterisation — thereby preventing false positives resulting from external attacks.

The system shall include logging and audit capabilities, ensuring that all connections, accesses and critical events are documented in the system with a minimum retention period of six months.

The Contractor shall have an incident response plan including specific procedures for managing cyberattacks targeting the service infrastructure. This plan shall include mechanisms for immediate notification to the Iberdrola IESE cybersecurity team (ciberseguridad_iese_ren@iberdrola.es) and the incident response team (srv-icsirt@iberdrola.es).

The Contractor shall ensure that all third parties and subcontractors involved in the supply, maintenance or support of the system comply with the same security controls undertaken by the Contractor.

The Client may request evidence confirming the implementation of security measures through external audits or penetration testing exercises.

Any contract with third parties shall include specific cybersecurity clauses covering the adoption of best practices in access management, data protection and incident notification.

All cybersecurity requirements annexed to this technical specification shall be complied with.

Any deviation from the stated requirements shall be approved in writing by the Client and for a defined period determined by the Client in such communication.