

Annex 7. HSE (Health, Safety, and Environment), Cybersecurity, and Biosecurity Requirements Host Site

Call 01 of 2026

BioEnergyTech Challenges Valle del Cauca

2026

1. HSE ECOPETROL S.A.

OBLIGATIONS OF THE PARTIES REGARDING HSE:

Each party (Host Partner and Cámara de Comercio de Cali) shall be responsible for compliance with the Health, Safety, and Environment (HSE) requirements and obligations contained in Colombian law, which shall extend to their workers, contractors, subcontractors, suppliers, visitors, and other beneficiaries or individuals using the facilities where the agreement is carried out. Therefore, each party must provide the necessary protection systems to keep its workers safe. Any legal instrument executed by virtue of this agreement shall include and comply with the same HSE (occupational health, safety, and environment) requirements of the agreement. In this regard, the Host Partner (hereinafter ALLY) is solely responsible for any breach of the obligations under its charge in this area.

The ALLY must have implemented an Occupational Health and Safety Management System (SG-SST) in accordance with the provisions of Colombian legislation. Said system consists of a logical, step-by-step process based on continuous improvement, which includes policy, organization, planning, implementation, evaluation, auditing, and improvement actions aimed at anticipating, recognizing, evaluating, and controlling risks that may affect safety and health at work. The SG-SST must be led and implemented by the ALLY, guaranteeing through said system the application of Occupational Health and Safety measures, the improvement of worker behavior, working conditions and environment, and the effective control of hazards and risks in the workplace. For this purpose, the ALLY must address the prevention of occupational accidents and diseases, as well as the protection and promotion of the health of workers and/or contractors, through implementation, maintenance, and continuous improvement. Said system must be extended to its workers, contractors, subcontractors, suppliers, visitors, and other beneficiaries or individuals using the facilities or carrying out activities under the agreement.

The ALLY will ensure compliance with preparation, response, and recovery activities in the event of any emergency that may arise during the performance of activities derived from the agreement, in accordance with the applicable legal framework.

The ALLY must inform ECOPETROL S.A and Cámara de Comercio de Cali throughout the entire execution period of any incident occurring within the facilities where the agreement is developed, in order to learn lessons and conduct investigations of said events for educational, preventive, and improvement purposes. Therefore, the ALLY shall be solely responsible for any consequences that may arise from the occurrence of an incident.

2. Challenge 1. Host Partner To Be Defined

2.1 HSE (Health, Safety, and Environment)

1. The personnel of the innovation team who will carry out the pilot test at the host company's facilities must meet the following requirements upon entry, previously validated and updated during the pilot execution:
 - Affiliation and payment to Occupational Risk Administrator (ARL), Health Insurance Entity (EPS), and Pension Fund Administrator (AFP).
 - All members of the solution team must have Personal Protective Equipment (PPE) for entering the plant. PPE for the development of the pilot test must be provided by the innovator.
 - The innovator's team must have a previously registered means of transportation to enter the plant.
 - The innovator's team must bring their own food and make use of the facilities provided for this purpose inside the plant, including the use of restrooms.
 - The innovator's team must establish the work schedule or working shift (Accompanied by the Supervisor / coordinator of the pilot test from the host company).
 - The innovator's team must allocate the necessary time on the first day for an induction in Occupational Health and Safety.
 - The host company, in agreement with the innovator, may monitor compliance with the HSE standards agreed upon with the solution provider.

- The host company operates 365 days a year from 6:00 a.m. to 3:00 p.m., during which operational support can be provided inside the plant for pilot coordination; conditions for operation during different hours will be evaluated. The host company does not have collective vacations.
- Equipment must be powered off when not in use to avoid risks during non-working hours.
- The external entity owning the equipment assumes full responsibility for any vulnerability originating in its hardware or software that could affect the host company's network.
- The pilot testing must prevent the generation of offensive odors into the atmosphere and employ all necessary mechanisms to mitigate them.

2.2 Cybersecurity

1. Software management and licensing:

- **Legality:** All installed software must have its respective valid corporate license. The owning entity is solely responsible for legal and technical compliance regarding these licenses.
- **Installation restriction:** The installation of unlicensed executables, "cracked" software, or personal/domestic licenses in corporate environments is strictly prohibited.
- **Equipment purpose:** Hardware must be used exclusively for technical project tasks. Use as a workstation for administrative, personal, or non-project-related purposes during collaboration with the host company is not permitted.

2. System security and data protection:

- **Antivirus protection:** Equipment must have an active corporate antivirus/EDR solution with updated signatures. The operating system must have the latest critical security patches installed.

- **Information transfer:** For data exchange, priority will be given to secure protocols: APIs with authentication, cloud services (corporate Google Drive), or email. The use of removable media (USB) is discouraged to mitigate malware risks.
- **Connectivity and network access:** Connection will be established via the host company's internal public network (Wi-Fi or wired), subject to coverage availability in the installation area.

2.3 Biosecurity:

The host company is a farm positive for Porcine Reproductive and Respiratory Syndrome virus (PRRS). Therefore, the innovator is required to ensure that:

- Team members have not entered other pig farms prior to entering the host company.
- A quarantine period of at least 4 days must be observed if they have visited other farms.
- Equipment and materials used on the farm should be for exclusive use within the agricultural company's facilities.
- Personnel must shower before entering the farm (at our facilities).
- Personnel must wear the footwear (boots) provided to them at the farm while on our premises.
- Biosecurity requirements and protocols may be expanded with precise guidelines to follow.

3. Challenge 2. Host Partner To Be Defined

3.1 HSE (Health, Safety, and Environment)

1. The personnel of the innovation team who will carry out the pilot test at the host company's facilities must meet the following requirements upon entry, previously validated and updated during the pilot execution:
 - Affiliation and payment to: Occupational Risk Administrator (ARL), Health Insurance Entity (EPS), Pension Fund Administrator (AFP).
 - All personnel must have industrial workwear/attire.
 - The innovator's team must have a previously registered means of transportation.
 - The innovator's team must bring their own food or make an agreement with the cafeteria service.
 - The innovator's team must establish the work schedule or working shift (Accompanied by the Supervisor / coordinator of the pilot test from the host company).
 - The innovator's team must allocate the necessary time on the first day for an induction in Occupational Health and Safety.
 - The innovator's team must undergo daily entry and exit access control by the host company. The host company provides ID badging processes.
2. **Energy management:** Equipment must remain powered on only during operating hours and testing. At the end of the shift, the person in charge must turn off the equipment to avoid unauthorized access risks during non-working hours.
3. **Custody:** The laboratory or pilot plant and its components will be supervised by a designated collaborator from the host company, who will act as a facilitator to ensure compliance with these best practices.

4. **Responsibility:** The external entity owning the equipment assumes full responsibility for any vulnerability originating in its hardware or software that could affect the host company's network.
5. **Odor management:** Pilot testing must prevent the generation of offensive odors into the atmosphere and employ all necessary mechanisms to mitigate them.
6. Working hours for the host company are Monday through Friday from 7:00 a.m. to 4:00 p.m. Operating outside these hours will require setting specific terms.
7. Between December 21 and January 10, 2026, host company personnel are on collective vacation. If strictly necessary, conditions to operate during this period will be evaluated.

3.2 Cybersecurity

1. Software management and licensing:

- **Legality:** All installed software must have its respective valid corporate license. The owning entity is solely responsible for legal and technical compliance regarding these licenses.
- **Installation restriction:** The installation of unlicensed executables, "cracked" software, or personal/domestic licenses in corporate environments is strictly prohibited.
- **Equipment purpose:** Hardware must be used exclusively for technical project tasks. Use as a workstation for administrative, personal, or non-project-related purposes during collaboration with the host company is not permitted.

2. System security and data protection:

- **Antivirus protection:** Equipment must have an active corporate antivirus/EDR solution with updated signatures. The host company reserves the right to validate protection status prior to connection.
- **System updates:** The operating system must have the latest critical security patches installed.

- **Information transfer:** For data exchange, priority will be given to secure protocols: APIs with authentication, cloud services (corporate Google Drive), or email. The use of removable media (USB) is discouraged to mitigate malware risks.

3. Connectivity and network access:

- **Network access:** Connection will be made through the host company's internal public network (Wi-Fi or wired), subject to coverage availability in the installation area. This network is isolated from the organization's critical servers.
- **Remote support:** Any remote access for technical maintenance must be supervised by the equipment lead at the host company and conducted through encrypted protocols previously authorized by IT (SETI).

4. Challenge 3. Host Partner To Be Defined

4.1 HSE (Health, Safety, and Environment)

1. The personnel of the innovation team who will carry out the pilot test at the Host's facilities must meet the following requirements upon entry, previously validated and updated during the pilot execution:
 - Affiliation and payment to: Occupational Risk Administrator (ARL), Health Insurance Entity (EPS), Pension Fund Administrator (AFP).
 - All personnel must have industrial workwear/attire.
 - The innovator's team must have a previously registered means of transportation.

- The innovator's team must bring their own food and may use the facilities designated by the Host for this purpose.
 - The innovator's team must establish the work schedule or working shift (Accompanied by the Supervisor / coordinator of the pilot test from the Host).
 - The innovator's team must allocate the necessary time on the first day for an induction in Occupational Health and Safety.
2. **Energy Management:** Equipment must remain powered on only during operating hours and testing. At the end of the shift, the person in charge must turn off the equipment to avoid unauthorized access risks during non-working hours.
 3. **Custody:** The laboratory or pilot plant and its components will be supervised by a designated collaborator from the Host, who will act as a facilitator to ensure compliance with these best practices.
 4. **Responsibility:** The external entity owning the equipment assumes full responsibility for any vulnerability originating in its hardware or software that could affect the Host's network.
 5. **Odor management:** Pilot testing must prevent the generation of offensive odors into the atmosphere and employ all necessary mechanisms to mitigate them.
 6. The **working hours** for the pilot test will be established by the Host from Monday to Friday. Operating outside these hours will require setting specific terms.
 7. **Environmental permits:** The external entity shall be responsible for complying with the following permits required by the Host: i) atmospheric emissions, ii) groundwater measurement, and iii) wastewater discharge measurement, where applicable.

4.2 Cybersecurity

1. Software Management and Licensing:

- **Legality:** All installed software must have its respective valid corporate license. The owning entity is solely responsible for legal and technical compliance regarding these licenses.
- **Installation Restriction:** The installation of unlicensed executables, "cracked" software, or personal/domestic licenses in corporate environments is strictly prohibited.
- **Equipment Purpose:** Hardware must be used exclusively for technical project tasks. Use as a workstation for administrative, personal, or non-project-related purposes during collaboration with the Host is not permitted.

2. System Security and Data Protection:

- **Antivirus Protection:** Equipment must have an active corporate antivirus/EDR solution with updated signatures.
- **System Updates:** The operating system must have the latest critical security patches installed.
- **Information Transfer:** For data exchange, priority will be given to secure protocols: APIs with authentication, cloud services, or email. The use of removable media (USB) is discouraged to mitigate malware risks.

3. Connectivity and Network Access:

- **Network Access:** Connection will be made through the Host's internal public network, subject to coverage availability in the installation area. This network is isolated from the organization's critical servers.

- **Remote Support:** Any remote access for technical maintenance must be supervised by the equipment lead at the Host.