

Privacy and Confidentiality Policy OSSA

1. Introduction

The Code of Ethics of UNDERGROUND WORKS S.A. (hereinafter, OSSA or the Company) acknowledges that the Company's activities may generate knowledge and commercial, technical, or any other information whose value largely relies on its confidentiality, and imposes discreet and professional use of the accessed information, maintaining due confidentiality.

Moreover, it ensures the confidential handling and privacy of third-party data held by OSSA. Lastly, OSSA commits to taking necessary measures to preserve the confidentiality of personal data in its possession.

2. Policy Overview

The aim of this Policy is to establish the requirements under which each member of the Company must handle information originating within the scope of the Company, safeguarding such information and preventing its unauthorized disclosure to third parties.

Under this Policy, the following shall be considered Confidential Information:

- ✓ Data of employees, clients, suppliers, and other third parties associated with OSSA, not publicly disclosed by the Company within legal boundaries and within the scope of its activities, or by the data owners.
- ✓ Documentation directly or indirectly influencing business development (technical procedures, offers, projects, studies, analyses, contractual documents, strategic plans, etc.), not publicly disclosed by the Company.
- ✓ Procedures, policies, instructions, processes, techniques, formulas, and all knowledge not publicly disclosed by the Company.
- ✓ Information from clients, suppliers, and third parties provided to OSSA under confidentiality agreements.

3. Scope

This Policy is applicable to all employees, executives, and members of OSSA's governing bodies, addressing both individual and collective actions performed by or on behalf of the Company.

It applies to all entities within the OSSA group, including subsidiary companies and temporary joint ventures (UTEs, joint ventures) in which the Company might have controlling interests.

This Policy encompasses all activities, processes, and relationships established by the Company and its employees at all levels, whether formally documented through contracts, policies, procedures, or similar means, or applied through customary or habitual practice.

4. General Requirements

Obligation of Discretion, Secrecy, and Confidentiality

The dissemination of confidential information, whether intentional or accidental, can cause significant harm to the Company's image, commercial stability, financial standing, and relationships with employees and affiliated third parties.

Therefore, to ensure information is used with the required level of secrecy and confidentiality, the following guidelines are established:

- ✓ All employees, executives, and members of governing bodies must adhere to the duty of discretion, secrecy, and confidentiality regarding Confidential Information within the scope of their job responsibilities or their involvement in different committees or groups within the Company.
- ✓ Confidential Information must be used for legitimate purposes in an honest and responsible manner, complying with the provisions of the Organic Law on Data Protection and other regulations ensuring information confidentiality.
- ✓ Compliance with confidentiality duties as stipulated in contracts with different clients, suppliers, and other associated third parties is mandatory.
- ✓ No employee, executive, or member of the governing bodies should, during or after their employment or business relationship, disseminate Confidential Information without OSSA's proper authorization.
- ✓ Immediate reporting to the Compliance Committee of:
 - Any use, dissemination, and/or publication of Confidential Information by other employees.
 - Any attempts by third parties not affiliated with the Company to obtain confidential information from any employee.

Measures to Ensure Confidentiality

- ✓ Inclusion of a confidentiality clause in contracts and agreements signed by the Company when applicable.
- ✓ Execution of a confidentiality document by contractors, subcontractors, consultants, and other individuals or entities external to the Company who have access to private and confidential information in the course of their work.
- ✓ Restricted access to information available on the internal computer network.
- ✓ Specific training for personnel handling sensitive confidential information within the Company.

In San Sebastián de los Reyes (Spain), on May 06, 2025
Mr. Carlos Puente Costales
President

