INFORMATION SECURITY, CYBERSECURITY AND ASSET SECURITY POLICY

COLBUN IS A LEADING COMPANY IN THE ENERGY MARKET. OUR PURPOSE IS TO TRANSFORM ENERGY, IN BALANCE WITH THE PLANET, TO FUEL YOUR PROJECTS AND DREAMS. ASSET SECURITY, INFORMATION, AND CYBERSECURITY RISK MANAGEMENT ARE CRUCIAL ACTIVITIES WITHIN OUR VALUE CREATION MODEL. THEREFORE, WE ARE COMMITTED TO IMPLEMENTING THE NECESSARY MEASURES TO PROTECT AND MITIGATE RISKS FROM THE DIGITAL WORLD WHILE SAFEGUARDING PEOPLE'S PHYSICAL SECURITY, OUR FACILITIES, AND THE ASSETS LOCATED WITHIN THEM.

THIS POLICY IS COMMUNICATED TO ALL EMPLOYEES, CONTRACTORS, DIRECTORS, AND SUBSIDIARIES. CONSEQUENTLY, EVERYONE IN THE COMPANY IS RESPONSIBLE FOR ITS IMPLEMENTATION AND COMPLIANCE.

1. CULTURE AND AWARENESS

- We recognize the risks associated with information security, cybersecurity, and asset protection. We are committed to fostering a culture that promotes the appropriate use of information, resources, and technology platforms. This commitment will be fulfilled through continuous awareness and training programs designed to provide employees with the knowledge, skills, experience, and capabilities required to uphold these principles.

- Information security, cybersecurity, and asset protection are shared responsibilities for both internal personnel and third parties interacting with the Company. Therefore, everyone must actively promote these practices in their daily activities, identify risks, and escalate alerts when necessary.

2. CONTROL AND PRACTICES IMPLEMENTATION

Individuals, management, boards, and committees that constitute the Company's information security, cybersecurity, and asset protection governance models must:

- Manage information security, cybersecurity, and asset protection risks by implementing identification, protection, detection, response, and recovery measures, and by assessing the vulnerability of systems.

- Notify the relevant management teams and adopt urgent recovery measures in the event of breaches or incidents that threaten information security, cybersecurity, or asset protection.

- Implement and maintain up-to-date verification, authorization, and access control technologies for the Company's systems and facilities. This includes logical and physical controls, applying the principle of least privilege required, and adhering to the principles of non-discrimination and good treatment outlined in our Code of Ethics and Human Rights Policy.

- Adapt swiftly to the evolving conditions of the information security and cybersecurity landscape and the protection of facilities. This will be achieved by leveraging processes and technological tools that enable rapid and innovative responses to the Company's needs.

- Comply with the requirements established in applicable legislation, regulatory standards, technical norms, policies, and internal procedures.

- Collaborate with relevant organizations, regulators, and industry associations to contribute to the global improvement of information security, cybersecurity, and asset protection practices.

José Ignacio Escobar T.

CEO Colbún

- This policy was approved by Colbún's Board of Directors on November 26, 2024.