INFORMATION SECURITY POLICY

Information Security is a central element to generate trust and a good reputation.
Our organization depends on flexible access to information and technology (IT) systems that support efficient work practices and help OPEX achieve its goals. OPEX intends to maintain a focused and effective information security function that follows recognized international standards, supports our core activities, and is optimized for security needs in our operating environment. Accurate, timely, relevant and properly protected information is essential for the successful operation of OPEX in its activities and in the provision of services to its clients.

OPEX is committed to protecting the Security of your Information. Provide the same commitment with the information entrusted to OPEX, its clients and shareholders, especially when it consists of information that is classified as industrial secret or copyright or is of a confidential, reserved, private, personal or relevant and sensitive nature, being that by the simple fact of knowing each other, a certain privilege can be obtained. OPEX will provide an information security management system that protects the confidentiality, integrity and availability of OPEX information.

The Information Security Policy applies to all forms of information, including, but not limited to, the following:

- o Talk, talk face-to-face, or communicate by phone, video, or radio.
- o Printed copy of the data printed or written on paper.
- o Information stored in manual file systems.
- o Communications sent by postal mail / courier.
- o Fax, email stored and processed through servers.
- o PCs, laptops, mobile phones.
- o Removable media, USB sticks, digital camera

To fulfill this commitment, we will:

- o Maintain an effective Information Security Management System.
- o Implement the most appropriate technology and infrastructure.
- o Create and maintain a security-conscious culture within the Security Services. information.
- o Continuously monitor and improve the effectiveness of the Safety Management System of the Information.

OPEX has the right to inspect all data that is stored, processed or transported in OPEX information systems, if necessary during operations, to comply with legal or internal information security demands or to carry out activities related to the worked.

As part of the Opex team, the information to which you will have access may be used as long as it is necessary, either directly related to the activities to be carried out due to the nature of the position, or if Opex so requires. If the above happens, it will be necessary to respect the information within
of the provisions of the laws in this regard, which protect confidentiality, and it will always be the obligation of every employee to protect the information.

n, the dissemination, disclosure, publication, disclosure, exchange, loan, reproduction, copy, extraction, obtaining, dissemination, appropriation or improper use of confidential information is prohibited. Electronic information must remain in the central IT infrastructure approved by the IT department. Such core infrastructure must be electronically and physically protected. Electronic information stored outside of this area (such as on laptops) must be backed up by the data custodian and encryption used where appropriate.

Management is responsible for ensuring that their direct reports understand the scope and implications of this policy. Violation of compliance is a breach of trust and will be grounds for disciplinary action.

Date:

Cesar A. Granados
chief executive officer
OPEX Perforadora SA de CV