Information security.

Important

Below we present the Rotoplas Group Information Security Policy, by clicking on the button:

“Marcar como completado”

you will be accepting the terms set forth in said policy.

Rotoplas® más y mejor agua	**Information Security Policy**	Policy code: GR-EAI-POL-014
		Date of issue: April 2021
		Review date: September 2021
		Review number: 02

PREPARED BY	**REVIEWED BY**	**AUTHORIZED BY**
Name: Maria de los Angeles Santiago Garcia Position: Security management	Name: Christian Sánchez Dominguez Position: Information Security and IT Manager Name: Ma. Del Carmen Garcia Romero Position: Senior manager MX, CA & LATAM conptrollership	Name: Diego Fernando Ponce Garcia Position: Transformation VP Name: Suraj Shinde Position: Digital and IT director Name: Luis Humberto Maya Marquez Position: Conptrollership Director

Policy objective

- To develop a framework for formulating and establishing rules and guidelines governing the handling of information and technological resources in Grupo Rotoplas to ensure the continued integrity, confidentiality and availability of the company's information.
- To align the functioning of the company's services and business activities related to information security.
- To ensure the continued trust of the company's customers, collaborators, partners and suppliers, shareholders and authorities by having a reliable and secure information system.
- To meet all the company's contractual, legal and regulatory obligations.
- To align the company's business strategy to ensure that it contributes to the fulfillment of the mission and vision of the Rotoplas Group.
- To establish and maintain a robust and sustainable information security culture in the company over the long-term.
- To effectively manage the company's information security risks by promoting continuous monitoring of new risks and following up on all corresponding mitigation plans.
- To assess the effectiveness of the controls in place in the company aimed at protecting the information handled by the business in accordance with the associated risks regarding confidentiality, integrity and availability.
- To mitigate the impact on the organization of incidents related to information security.

Policy scope

This policy shall be applicable for all Grupo Rotoplas personnel who work for or provide services to the company, as well as the company's investors and subsidiaries, which this policy must be followed to ensure the confidentiality, integrity and availability of the company's information.

Policy description

Founded in 1978, Grupo Rotoplas provides residential and commercial water storage, piping, purification and treatment solutions.

At Rotoplas, our mission is to bring more and better water to people, which is why we have spent the last forty years striving every day to create the best residential and commercial water storage, piping, purification and treatment solutions. We are a leading Mexican company with a long history of providing the best water solutions to our customers in Mexico and across the Americas.

Grupo Rotoplas has decided to take actions aimed at strengthening the company's information security to protect the organization's assets into the future. These actions are aligned with leading best practices.

Grupo Rotoplas understands that its information assets, which rely on its technological infrastructure, are essential for the execution of its strategy and for the continuity of the business so that it may fulfill its mission and vision.

Grupo Rotoplas is committed to its continued compliance with all standards and requirements related to information security and the confidentiality, integrity and availability of its information assets.

Grupo Rotoplas is also committed to implementing, operating, monitoring, reviewing, maintaining and continuously improving our information security management efforts to ensure that the controls that we select for implementation effectively protect our information assets and provide certainty to our customers, suppliers, employees, shareholders, regulators and all other stakeholders.

Terms and Glossary

- Information asset
  Any tool, device or program that is handled by the company's people or which contains information of value for GRUPO ROTOPLAS.
- Confidentiality:
  Characteristic whereby information shall not be disclosed to unauthorized persons or systems. Confidentiality means that access to information shall only be given to individuals who have the appropriate authorization.
- Control:
  Ability to exert or direct influence over a given situation or event. It is an action taken to bring about circumstances that are aligned to a specific plan.
- Availability:
  Characteristic, quality or condition whereby information is available to the people, processes or applications who need to use it. It is access to information by authorized persons whenever they need it.
- Strategy:
  Set of decisions that are made to determine the organization's policies, mission, vision and objectives. Information
- Information
  Organized data generated by the application of business solutions. Written information such as procedures, manuals, contracts, etc.
- Integrity:
  Characteristic of information whereby no unauthorized changes may be made to it. It means that information is maintained in its exact original state, without being manipulated or altered by unauthorized persons or processes.
- Rule:
  The way in which a procedure or process is carried out.
- Risk:
  Probability of the occurrence of a particular event and the consequences of that event.
- Information security:
  Maintaining the confidentiality, integrity and availability of information.
- Username:
  Grupo Rotoplas employee or other persons that provide services to the company and who, due to their roles, are authorized to access and use the company's technological solutions.

Internal Control Objectives

- Financial Reporting - reliability of information
- Operations - continuity of the organization's operations
- Compliance - with internal rules and the laws and regulations to which the organization is subject.

Policies

Responsibilities regarding information security and the systems that handle, store and transmit it extend to all levels and functions of the Rotoplas Group.

Senior management is responsible for establishing the information security objectives of the Rotoplas Group and for ensuring that those objectives are aligned with the organization's overall information security strategy.

Information Security Committee

The company's Information Security Committee shall be in charge of making all decisions related to the information security strategy of the Rotoplas Group.

The Committee shall meet at least once a year or whenever required to do as the result of an exceptional event.

The Committee shall be comprised of at least the following individuals:

Directors of stakeholders
Digital and IT director
IT senior management staff
IT and information security manager
Infrastructure manager
Controllership manager
Corporate security manager

Head of information security

The information security officer of the Rotoplas Group shall consider:

Implementing an information security strategy that ensures the company's compliance with the basic principles of this policy. The information security officer shall direct the protection of the company's information assets and promote the company's overall information security culture as an administrator of the company's Information Security Management System (ISMS), in conjunction with all the organizations's personnel.

The company has in place a responsibility governance control model that is reflected in the following roles:

- Process head: Person assigned to ensure that the end-to-end process is effective and efficient.
- Control head: Person assigned to execute the control or activity comprising a process.

Responsibility of personnel

It is the responsibility of all personnel to know and adhere to the company's policies, procedures and Code of Ethics; Any breach of these rules and regulations shall be acted upon following the guidelines described in the Code of Ethics and any applicable laws.

- All individuals who provide services to the Rotoplas Group must know and comply with the Policy and they shall maintain the professional secrecy and confidentiality of any and all information they have access to as part of their professional activities.
- All personnel shall be responsible for the security of the information that their roles involve.
- Said individuals shall communicate, on an urgent basis and following the established procedures for doing so, any potential security incidents or problems that are detected.

Awareness, education and training

- Company personnel must participate in any courses required by the Rotoplas Group.
- All personnel of Rotoplas Group and third-party users who provide services to the company must participate in awareness activities, courses and periodic training on information security matters.
- All Rotoplas Group personnel must know the company's Information Security policy and be certified on the policy.
- All third parties that provide services must know and adhere to the guidelines of the Information Security policy.

Use of Assets

- The assets of the Rotoplas Group must be used and handled properly to prevent the unauthorized disclosure, modification, withdrawal or destruction of company information.
- All personnel must take care of the assets that have been directly allocated to them or to which they have been granted access.
- All personnel must connect their work tools exclusively to secure networks.
- All personnel and external users must return company assets that they possess to the company at the end of their employment or contract with the Rotoplas Group.
- All information related to operations in the organization must be stored, handled, shared and communicated exclusively using company equipment authorized and assigned to the individual in question by the Rotoplas Group.

Access control and use of passwords

- Each employee is responsible for all actions taken using company equipment accessed via his or her credentials.
- All personnel who have access to company systems should have a unique and personalized username.
- All users must be authorized to access company systems and they shall have access to company resources with the minimum of level of privileges required to carry out the actions corresponding to their work roles.
- System accounts and passwords must be closely safeguarded by the responsible person in charge and must not be shared for any reason.
- Users who have been assigned a password by a third party must change that password the first time they connect to company systems.

- Whenever users have reason to believe that their password might have been compromised, they should immediately change their password.
- Passwords should be treated as confidential and privileged information.
- Passwords should not be written out in electronic or printed communications.
- Never write down your password on documents or paper of any kind and never enter your password on public or shared computers or computers whose level of security is unknown.
- Company personnel should avoid using their browser's "remember password" option, particularly on shared computers.
- Passwords must comply with the following rules:
  - Passwords made be at least eight characters long.
  - Passwords should be changed every three months.
  - Passwords must contain at least one number, one letter, one uppercase letter and one special character.
  - Users may not re-use any of their last five previously used passwords.

Transfers of information and use of portable storage devices

- Company personnel should use the internet appropriately for what is required for their specific roles.
- Connecting or installing devices and software not authorized by the Rotoplas Group is strictly prohibited.
- The use of mobile storage devices, such as CD/DVD disc burners and portable memories (USB, SD, MMC, Micro SD, etc.) or any other storage medium or device that threatens the confidentiality and availability of the company's assets, is strictly prohibited.
- Only company information should be stored in mobile storage devices assigned to company personnel, in accordance with the attributes and functions of each employee's position.

Physical security in the facilities

- All visitors to the facilities of the Rotoplas Group must sign in and be authorized for entry.
- All suppliers, external personnel and other visitors must be authorized for entry into company facilities and must be accompanied by the responsible individual from the Rotoplas Group.
- Outside individuals who perform work inside company facilities must be supervised by personnel of the Rotoplas Group.
- Access to restricted areas shall be limited to persons authorized by the responsible individual of the Rotoplas Group.
- Entry/exit controls
  - All individuals who wish to enter the offices, plants and facilities of the Rotoplas Group must sign in (name, surname, arrival and departure times, etc.) before doing so. and said outside persons must be accompanied at all times during their stay in company facilities until their departure.

All company personnel shall adhere to the control procedures put in place by the Corporate Security area and any other access controls set forth in the security procedures of the Operations Manual and instructions for plant personnel.

Operational safety

- The use of unauthorized software is prohibited.
- Company personnel should refrain from opening emails and URL links from unknown senders.
- Third-party computers that are authorized to connect to the company's network should have an antivirus program installed in them and should have all appropriate security features.

Clean desk and unattended computers

- Company personnel should take steps to ensure that the physical and digital documents that they possess, and which contain confidential and/or privileged company information are not visible or accessible on their computer screens, workstations or storage media.
- Never leave your computer unattended and be sure to put your computer in sleep mode if you leave your work area for whatever reason.

Responding to information security incidents and anomalies

- Any behaviors or actions that threaten the information security of the Rotoplas Group should be reported to the following email address: infosec@rotoplas.com.

All company personnel and outside parties must adhere to this Policy and the annex to the information security policy, which describes the controls that must be implemented and followed to ensure the confidentiality, integrity and availability of company information. These controls are categorized as follows:

A. Information security policies
B. Information security structure
C. Human resource security
D. Asset management
E. Access control
F. Cryptography
G. Physical and environmental security
H. Operational security
I. Communications security
J. Information systems acquisitions, development and maintenance
K. Supplier relationships
L. Information security incident management
M. Information security related to ensuring business continuity
N. Policy compliance

Consequences of policy violations

- The Ethics Committee of Grupo Rotoplas shall be responsible for determining the occurrence of information security incidents and/or violations to this policy and for disciplining the personnel involved in any such breaches, as set forth in the Code of Conduct and Ethics, as well as the model of recognitions and consequences.

Exceptions

- All exceptions to this policy must be formally requested by the director of the area seeking the exception and duly authorized by the controlership director and digital and IT director. Policy exceptions should be supervised by the head of information security of Grupo Rotoplas.

This document must be reviewed and updated at least once a year or whenever significant changes are made to the infrastructure and/or critical operations of the Rotoplas Group.

Sources of information and references

This Information Security Policy is based on ISO 27001 and NIST.

Forms/Annexes

- GR-EAI-POL-010 Password Management Policy
- GR-EAI-POL-011 Policy Regarding Acceptable Use of Assets and Responding to Business Communications
- GR-EAI-POL-013 Policy Regarding the Use of Computer Equipment, Communications and Social Media
- GR-EAI-POL-016 Policy Regarding the Use of SAP Accounts for External Consultants
- GR-EAI-MAN-003 Specific Information Security Principles Manual
- GR-CAP-PRO-003 Supplier Assessments

CHANGE HISTORY

Policy review number	Policy review date	Description of the Change
00	April 20, 2021	Document created
01	June 25, 2021	Change in authorization box / policy title / wording of the more general policy / the password guidelines were added.
02	September 01, 2021	The model of recognitions and consequences in sanctions was added. Adjustment in approval