Rotoplas®

Information security.

Important

Next we will present you the
Grupo Rotoplas Information Classification 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 Classification Policy**	Code: GR-EAI-POL-020
		Fecha de emisión: September 2021
		Fecha de revisión: September 2021
		Revision No.: 00

PREPARED BY	**REVIEWED BY**	**AUTHORIZED BY**
Name: Maria de los Angeles Santiago Garcia Position: Head of Security Management	Name: Christian Sanchez Dominguez Position: Information and Technology Security Manager Name: Laura Jimena Silva Position: Data Governance Manager Name: Ma. del Carmen Garcia Romero Position: Sr. Manager MX, CA & LATAM Comptrollership	Name: Diego Fernando Ponce García Position: VP of Organizational transformation Name: Suraj Shinde Position: Director of Digital & IT

Goal

Establish the guidelines for the classification of information according to its sensitivity or degree of impact on Grupo Rotoplas and indicate the security requirements that must be met in terms of identification, labeling, access, storage, reproduction, distribution, and destruction of the information, depending on its level of classification.

Scope

This policy is applicable to all information produced, obtained, held, or controlled by Grupo Rotoplas, regardless of the medium in which it is handled.

Description

This Policy is based on the classification of Grupo Rotoplas' information so that any information that requires a higher level of protection is duly identified and the corresponding security measures are taken, to safeguard confidentiality, integrity, and availability.

Terms and Glossary

- Information assets: Refers to any information or element related to its treatment (systems, supports, buildings, people) that has value for the organization.

- Classification of Information: It is the classification that must be given according to the legal requirements, value, criticality, and susceptibility to unauthorized disclosure or modifications.

- Integrity: The property to protect so that assets are accurate and complete.

- Availability: Information should be easily accessible to people who need it.

- Confidentiality: Ensure that information is only accessible to authorized persons.

Internal Control Objectives

- Financial Reporting – Reliability of Information
- Operations – Continuity of the organization's operations
- Compliance – with internal rules, laws, and regulations that affect the organization.

Policy

- Classification criteria:
    - The information assets managed and in the custody of Grupo Rotoplas will be identified, classified, and managed in terms of their confidentiality, integrity, availability, impact, value, and criticality.
    - That internal laws, regulations, policies, and processes are complied with.

- Roles and responsibilities:

    - The Information Security department is responsible for ensuring that the guidelines of this procedure are complied with.
    - All employees are responsible for:
        - Complying with this Policy.
        - Safeguarding the confidential or privileged information of Grupo Rotoplas.
        - Ensuring the proper treatment of the information during its life cycle (creating, collecting, using, treatment, transmitting, sending, transporting, storing, and final disposal (destruction)).
        - Complying with the security controls established according to the level of classification of the information.
- Classified documents must bear a legend indicating the type of classification of the information.
- Declassify or reclassify; the owners of the information generated should review the level of confidentiality and should assess whether that level can be changed.
- People who possess confidential or privileged information are prohibited from:
    - Disclosing or entrusting information to other unauthorized persons.
    - Make improper use and benefit, directly or indirectly, personally or for third parties, from confidential or privileged information. The misuse of such information may have civil or criminal consequences, regardless of the disciplinary action established by the Company for these cases.
- Physical information classified as confidential must be secured under lock and key in cabinets (they must have a label), drawers, or sites that guarantee its protection.
- To recycle physical paper, it must not contain confidential and privileged information.
- In the event that, for business reasons, confidential and privileged information must be provided to third parties, an authorization must be obtained from the person responsible for the information, data governance department, and the Information Security department.
- It is forbidden to talk about privileged and confidential information in public places such as airports, elevators, etc.

- In case of any fortuitous (accidental) or deliberate situation that compromises the security of the information, the employee must report it immediately, through a phone call, message, or email to their immediate superior. Likewise, they must report to the email address infosec@rotoplas.com

Classification of Information

Level	Definition	Treatment	Criticality
Privileged	All information related to events that can influence the company, such as prices or trends, as long as such information is not made public. (Examples: codes, formulas, business practices, and pricing schemes).	Access restricted to only senior management or a few key people and whose disclosure has a critical negative impact. Note: Disclosure has a serious impact on long-term strategic objectives or puts the survival of the organization at risk.	If the level of information is privileged and its availability is medium or high, the criticality level will be **Critical.**
			If the level of information is privileged and its availability is low, the level of criticality will be **High.**
Confidential	Confidential use information is all information related to the business (such as new product strategies, business plans, financial data, personal data, etc.) of Grupo Rotoplas.	Area directors and key employees have access and its disclosure has a high negative impact. Note: Disclosure has a significant short-term impact on operations or tactical objectives.	If the level of information is confidential and its availability is high, the criticality level will be **Critical.**
			If the level of information is confidential and its availability is medium or low, the criticality level will be **High.**
Internal	The information for internal use is that which is generated based on the daily operations that are carried out between people or areas of Grupo Rotoplas (Reports, Presentations, e-mails, directories, web portals, policies, etc.)	Relating to information accessible only to members of the organization, but at any level and whose disclosure has a medium negative impact Note: Disclosure causes minor inconvenience or minor operational inconvenience	If the level of information is internal and the availability is medium or low, the criticality level will be **Medium.**

Public	Information for public use (public) is all information that is disclosed to the mass media, or through channels established by Grupo Rotoplas (campaign brochures, public statements, job publications, etc.). Everyone, inside and outside the organization, has access.	Everyone, inside and outside the organization, has access. Note: Disclosure does not cause any harm.	All public information is considered to have low **criticality**.

Sources of Information and References (when applicable)
ISO/IEC 27001 standard
GR-EAI-POL-014 Information Security Policy
GR-EAI-MAN-003 Manual of Specific Information Security Principles Jun 2021 Rev. 00

Sanctions

The Ethics Committee of Grupo Rotoplas will be in charge of assessing and sanctioning employees' participation in incidents and/or information security violations related to this policy, aligned with the Code of Ethics and Conduct, as well as the Consequence and Recognition model.

Forms/Appendices
GR-EAI-PRO-010 Information Labling Procedure

The revision or updating of this policy must be carried out as required, or at least once per year.

RECORD OF CHANGES		
Revision Number	**Revision Date**	**Description of the Change**
00	September 2021	Creation of document.