INFORMATION SECURITY POLICY

Policy	**Executive in charge:**	**Contact person:**
Finance Management	Chief Financial Officer	Deputy Director of Information Services IT Infrastructure & Operations Manager

OBJECTIVE:

It is policy of Kimberly-Clark de Mexico that all employees are responsible for taking care of and safeguarding the technological infrastructure to protect the company's information and that employees who, for reasons of their work, have access, manage, or prepare sensitive or confidential information, are responsible for the custody, use, disposition or destruction of it.

SCOPE:

Applies to Kimberly-Clark de Mexico and Subsidiaries, hereinafter KCM.

DEFINITION:

Information security is defined as protecting, safeguarding, caring for, and managing the information prepared or stored in any way, whether paper, systems, computers, laptops, cell phones, servers, the Cloud, to prevent any person, unauthorized or unrelated, from having access to KCM information and that could disclose or use and cause any damage to KCM.

RESPONSIBILITIES

1. The Chief Executive Officer is a member of the Board of Directors and is responsible for informing senior executives of decisions taken by the Board of Directors that have an impact on economic, social, environmental, technological, and cybersecurity issues. In turn, senior executives make the relevant decisions and communicate them to employees.

2. The Information Services Management is responsible for identifying the Technological and Cybersecurity risks, and if any, they are included in the risk portfolio, they are

evaluated, and mitigation measures are implemented, in addition, KCM has Policy no. 60 "Crisis Management and Business Continuity Plan".
The IT Department will be responsible for planning, executing, and following up on the requirements addressed to KCM staff, as well as the fulfillment of the courses on topics of Information Security / Cybersecurity.

3. It is the responsibility of each Director / Deputy Director / Comptroller / Leader / Manager to establish and verify protection controls:
   a. To identify and classify information that requires special management and care.
   b. To determine who should have access, to what type of information, and how classified information should be managed.
   c. To determine who and how classified information should be moved from one site to another.
   d. To instruct staff to refer all received external requests for classified information to the Director / Deputy Director / Comptroller / Leader / Manager of their department for express approval prior to providing any data.
   e. To instruct staff to avoid talking to other people about the company or its work plans, in public places, such as: elevators, taxis, airplanes, waiting rooms, restaurants, clubs, among others. Also, to take care of the comments made about the company with family and friends.

4. It is responsibility of all KCM employees to report to their immediate superior the issue that could put KCM at risk regarding Information Security and Cybersecurity and this, in turn, will report it to the Director / Deputy Director / Comptroller / Leader /Manager and will attend to the indications of the Information Services Department.

INFORMATION PROTECTION AND CLASIFICATION

Information should be classified as follows:

- **Public:** Routine operational information, such as public reports or product general descriptions.
- **K-C Internal Use Only:** Default category, such as address lists or general reports.
- **K-C Confidential:** Valuable data, such as intellectual property (formulations or product brand information, among others), customer lists, sales information, customer pricing and discounts, prices and volumes of raw materials, and materials.
- **K-C Sensitive:** Information subject to legal requirements, such as medical or social security records.

AUTHORIZATION

The Director / Deputy Director / Comptroller / Leader / Manager of the department, as applicable, are the only ones who can authorize employees, who, for reasons of their work, must have access to the information classified as confidential of their department.

MANAGEMENT

It is responsibility of the user of the confidential information that this is not visible or accessible, due other people outside the function, or the company can obtain data about it.

The information should be kept in a safe place and/or removed from the computer and/or laptop screen when someone is near its place and block it when the user leaves the work area.

Whenever sensitive information is moved through any electronic device, it must have the corporate authorization to do it.

STORAGE

The user of confidential information contained on paper should ensure to kept it in a locked place when it is not in use. Likewise, to make sure that the correct custody is taken when the office is leaved.

It is the responsibility of the Director / Deputy Director / Comptroller / Leader / Manager to request an advance backup of the information contained in the PCs / Laptops /Cell phones assigned by the company to the employees who will cease to provide their services in the company, by requesting it to the Information Technology Department.

Important: The use of ***personal computers, tablets, and cell phones*** for sending or storing company information is prohibited; storing and/or backing up company information on external devices, such as USB disks or USB flash drives, is prohibited too.

ELECTRONIC SYSTEMS

Users of personal computers must have a password to start their computers, as well as to protect confidential information. E-mail (Outlook) can be used to send confidential information to other KCM locations, if it is authorized by the Director / Deputy Director / Comptroller / Leader / Manager of the department to perform this activity.

The password to access computers and communication systems should never be given to another person.

PCs / Laptops / Cell Phones should never be left within reach of other people and should be stored in a safe place.

DESTRUCTION / DELETION OF FILES

Once the information retention period has ended, the Director / Deputy Director / Comptroller / Leader / Manager or any person who manages confidential information must request authorization from the Tax Management and the Corporate Comptroller's Office to proceed with the destruction or deletion of files.

When confidential paper information is no longer useful, it should be destroyed using a paper shredder and deposited in the paper bins.

Electronic devices must be disabled by splitting them into several fragments. In the case of PC / Laptop / Cell phones hard drives, the IT Department is responsible for formatting them to remove the information they contain.

For the information stored in the Cloud in "OneDrive", "Outlook", "Share Point", among others, the Director / Deputy Director / Comptroller / Leader / Manager must request IT, in coordination with Human Resources, for backups before the person stops working in the company.