CORPORATE POLICIES

INFORMATION SECURITY POLICY

INFORMATION SECURITY FRAMEWORK

INTRODUCTION

All of Prodeco Group's information systems and the data therein stored, independently from its location, are property of the Prodeco Group. The Data and Information Systems are vital resources and must always be used in a responsible manner.

Information and Information Security

Information is fundamental for all our business areas and support functions.
We recognize that such information:

- Varies in importance and sensitivity for the Prodeco Group, and
- Exists in electronic, printed or verbal manner.

Any information generated or exchanged in the course of Prodeco Group business or that in any manner has been stored, processed or transmitted within Prodeco Group systems is considered information belonging to the Prodeco Group and is governed by present policy.

The security of the information, by extension, is also considered fundamental for the Prodeco Group; it includes the practices that ensure that the information about our business is understood, protected and is available to the appropriate persons at the right moment.

Our Commitment

We recognize that the security of the information is an important aspect of the business, through:

- Compliance of all applicable laws and regulations;
- Granting authority to our Information Technology Teams (ITT) so that they can be facilitators of information security; and
- Providing our users the necessary resources to work in a safe manner.

The objective of this policy is to guarantee that all of us will become aware of the risks facing the information of Prodeco Group business, understand our obligations and understand the consequences of not adhering to this Policy.

Who should comply this policy?

This Corporate Policy is part of the Prodeco Group Corporate Practice Framework and applies to all the operations with controlling interests, or that are directly or indirectly managed by the Prodeco Group. Each employee or contractor that works for the Prodeco Group, without regard to his or her role or location, must comply with this policy.

In the Joint Ventures companies in which we are not the operators, we must try to influence our associates so that they adopt similar policies and procedures, whenever possible. Each one of us must take reasonable measures to ensure that other persons or external groups associated to the Prodeco Group will proceed in the same manner.

THE SCOPE OF INFORMATION SECURITY

Our concerns

We recognize that the sector is susceptible to experience a series of threats and by virtue of our profile we are an objective in the geopolitical frontier. We also observe a series of IT trends that are modifying the risks that we face:

- **Greater IT connectivity:** for our systems, employees and external associates; and
- **A more complex IT environment:** with the blurring of personal and labor boundaries.

Even though we continue taking advantage of information technologies for our business and to connect with colleagues and global associates, we must be cautious with regards to the origin of security threats, for example:

- **Within the company itself:** the users that try to perform their work with good intentions, but not always in the most appropriate manner, or opportunistic persons that abuse the access granted.
- **From outside of our organization:** from attackers increasingly more sophisticated, who are gradually organizing themselves better and using better tools and/or techniques in search of economic, political and social gains.

Protecting Prodeco Group's information
Information security consists in recognizing the threats and identifying and protecting our IT assets. For the Prodeco Group such assets include:

- **Prodeco Group information:** that exists in a series of business systems, supported by IT networks and communication infrastructure; and
- **Our People:** we have experts in key roles throughout all our operations, covering marketing to industrial and administrative positions, and we must protect the practical knowledge of the business that these persons have.

Classification of the information
To better protect our computer assets we have established the following classification for Prodeco Group information:

- **Strictly confidential:** includes internal information (vital in terms of time) of the business or personal data, whose disclosure can affect the value of Prodeco Group companies or the privacy of its employees. For example the information can address possible mergers or company acquisitions (and associated information), anticipated disclosure of financial statements and employee's documentation.
- **Confidential:** information shared within and among the divisions or internal teams to comply with our regular business tasks. Comprised by the set of internal information of private and reserved character (not public), which must be protected. For example customers and partner's information and systems technical information.
- **Public:** information neither Strictly Confidential nor Confidential or that is already in the public domain, such as financial statements and the information found in our public web site.

You must be aware that certain business information is more sensitive than another and we must take the necessary steps to protect it. Additionally, our information security approach must address the different security risks faced by our employees, whether they are management, final users, third parties or belong to the IT area.

OUR MECHANISMS TO PROTECT INFORMATION

This Information Security Policy is supported by a deeper IT security environment and is part of the Prodeco Group Corporate Practices Governability Framework. It is aligned with Our Values as well as with the Code of Conduct. Such documents must always be considered as our Fundamental Principles.

Information Security is endorsed by other corporate and local policies, for example those that address retention, corruption and privacy of information, among other considerations. The implementation of site security includes local procedures associated with ownership and responsibility to efficiently carry out the security activities throughout the business.

PRINCIPLES OF THE INFORMATION SECURITY FRAMEWORK

Our approach is based on simple principles regarding information security:

1. **Prodeco Group's information must be protected.** The knowledge of the business influences success, and information access must be based in the "need-to-know", under adequate protection levels.
2. **Information security must be relevant and simple.** It must not hinder business by being too complex, costly or not practical.
3. **We expect our employees to act responsibly.** We endorse this premise with simple and clear policies, a strong management and pertinent training for understanding IT risks and for how to use technology in an effective manner.

When applying these principles in a collective manner, we can ensure that the processes and tools stipulated within our framework are appropriate to all the levels of the business.

Our Information Security Framework
This policy is the foundation for Prodeco Group's Information Security Framework that is applied throughout the whole organization. It ensures the application of uniform and effective controls to protect our global information assets. The bases for the Information Security Framework are:

Responsibilities
Each person is individually responsible for the security of Prodeco Group's information. Every employee, consultant, contractor or associate

with access to our computer systems must comply the corresponding IT Service Agreement. Additionally we must be aware of and support the following security functionalities:

- **The Owners of the Information and Systems:** The Prodeco Group has roles that are responsible for the custody of key data and systems. Such roles allow the understanding of the risks associated with systems and support the technologies and processes necessary to secure data.

- **IT teams:** Many controls of the Prodeco Group Information Security Framework are directly configured in our IT systems and support processes. Your local Help Desk and IT Manager are security facilitators and must be the first point of contact regarding any consultation or IT security situation.

- **Other internal control functionalities:** Human Resources, Legal Department, Regulatory Compliance and Internal Audit have specialized knowledge and also work together with the IT teams to guarantee Prodeco Group's information security.

Technologies and Processes

Prodeco Group's information security also depends on business technologies and processes. To guarantee the security of our IT environment it is necessary to have specialized systems and configurations, and their maintenance and supervision being essential. We all have the duty of supporting the implementation of technical and process controls established by the IT teams and to reduce to the minimum the risks faced by the information assets.

Our security processes are widespread and are also centered in our people, through simple and efficient training courses regarding information security. This is a requirement recognized by the Prodeco Group Business Practices Committee and implemented locally, which reinforces the security position of the Prodeco Group.

Presentation of concerns regarding information security

In spite of the efforts carried out, it is possible to face situations that can affect the security of our information assets. In such cases, your concern must be presented to your local IT area.

If your concern is broader, you should communicate with your supervisor or immediate manager or any other corresponding manager (human resources, legal or top management). If your concern has not been resolved, please refer to section "Presentation of Concerns" of the Prodeco Group Code of Conduct.

Consequences of Non-Compliance

The lack of compliance of this policy, of the corresponding IT service agreements, or of the general Information Security Framework exposes the Prodeco Group to business risks that could result in important financial losses, affect its prestige and (in the operations) cause injuries and diseases to personnel.

The lack of compliance may generate disciplinary sanctions, such as for example termination of the labor contract or of third party contracts, and personal consequences, such as judicial actions and/or criminal investigations.

However the active support of this Policy and its implementation within our Information Security Framework can reduce the collective information security risks that we face; and ensure the continued success of the Prodeco Group in a world increasingly connected through electronic means.

Mark McManus
CEO