INFORMATION SECURITY POLICY

This Policy for Information Security establishes the general principles against which to set out the organizational requirements to attain, and maintain, the Information Security.

Premise

For "Information Security" shall mean the condition in which an organization is able to pursue and maintain over time, a level of confidentiality, integrity and availability of information to comply with the requirements established by:

a) Current legislation (in particular the protection of privacy and intellectual property);

b) Customers' contractual requirements;

c) Any additional requirements established independently by Palladio Group.

The "confidentiality" indicates the information characteristic of not being accessible to unauthorized persons; the "integrity" of information indicates the information characteristic not to be editable, or erasable, except by authorized persons; and the "availability"indicates the information characteristic to be accessible at the request of an authorized person, within certain time.

Generality

Palladio Group has the need, as part of its business operations, to access to, and process in various ways, information that may relate to: Customer projects, personal data of employees and collaborators, administrative and accounting data produced and retained for the purposes to comply with legislative requirements.

The Palladio Group Management believes, in this regard, that the adoption of an organizational model aimed at information security is a strategic decision and needed to put the organization in a position to:

a) Produce, use, and properly store the information needed to comply with regulatory or contractual obligations;

b) Efficiently use the available resources, through a suitable classification of critical information;

c) Generate and maintain over time, the confidence of the Palladio Group stakeholders against the Company reliability in protecting the information that it generates and uses.

PRINCIPLES

The Information Security is a strategic decision

Awareness of the importance of generating, using and storing the information correctly has to become part of the daily work at all levels. Ideally all decision-making and executive processes of Palladio Group which involve the production, access and processing of information, must be structured so as to pursue the security of such information.

Information security is based on a risk approach

In pursuing information security there are no "magic formulas" or "best practices" applicable to any situation: the way the company deals with information security is closely linked to the threats and opportunities the organization believes to be exposed to. The discipline of risk-based thinking is the tool that helps to identify and give proper priority to the various threats and opportunities: this tool should then become part of the daily work for all decision making parties in Palladio Group.

Information security starts by following the rules

To ensure the security of information is vital to have a focus on knowledge, and respect,of the legislative and contractual requirements. If in general the decisions on security of information should be taken with a risk-based approach, ie through an evaluation of costs and benefits, legislative and contractual requirements should always be considered a "pure risk", namely only as a source of threats (related to non-compliance with legislation or contractual clauses) and never as an opportunity. The organization must therefore commit, to all levels in identifying, understanding and complying with legislative and contractual requirements for information security.

Specifically, there must be an awareness at all levels of the organization that the organizational model adopted by Palladio Group for information security is defined and implemented in accordance with UNI CEI ISO / IEC 27001: 2014. Therefore, at various organizational levels is required awareness of the requirements of that Rule and the importance of their respect.

Information security needs to work towards goals

To have adequate confidence that information security will be achieved and maintained over time it is necessary to set a path, marked by the presence at the various organizational levels of appropriate targets. If the definition of the specific content of the objectives is left to the various levels of management, in general it is necessary that these objectives are:

a) Expressed in measurable terms, as far as practicable;

b) Compatible with and proportionate to the resources available to the Organization;

c) Accompanied by appropriate deadlines, in the absence of such an objective can not be regarded as such;

d) Monitored periodically.

Information security is a continuous improvement

The Organization's framework (the market, the company, the needs and expectations of customers, ...) changes continuously. In this condition it is impossible for any organization to be likely to survive, if it doesn't regularly question its values and its practices in order to ensure that this are still appropriate for addressing the changes that inevitably it has to face.

Chief Executive Officer
Dr. Mauro Marchi

Mauro M