Information Security Policy (ISP)

Prepared by:	Passio Consulting

Document Version History

Version	Preparation date	Prepared by	Approved by	Change management
1.0	20/12/2017	Passio Consulting	Paula de Oliveira	Initial version

Agenda

Information Security Policy Objective 4

Information Security Policy Scope 5

Information Security Policy Principles 6

Information Security Policy Responsibilities, Maintenance and Communication 7

Information Security Policy Objective

Passio Consulting's Information Security Policy has the objective of being a common understanding to all stakeholders, allowing protection against unauthorized use or access to information, while the integrity and confidentiality of such information is preserved, through the adoption of effective practices in the management of information security.

Information Security refers to the protection of the information of a particular company or person, applying both corporate information and personal information.

Passio Consulting top management is committed to adopting compliance mechanisms with the applicable legal requirements in the context of Information Security.

Information Security Policy Scope

Passio Consulting's Information Security Policy is intended for all employees, trainees and service providers. Everyone must comply with the Information Security Policy and the documents related to Information Security and Privacy.

Employees, trainees and service providers who deliberately violate this or other policies are subject to disciplinary actions, which may go as far as the termination of their contractual relationship with Passio Consulting, and these situations will be participated to judicial authorities and treated as potential crime.

Passio Consulting's information security policy is based on the following attributes:

Confidentiality: guarantee that the information is accessible only by persons duly authorized for this purpose;
Integrity: guarantee information accuracy and its handling, maintains all the original characteristics;
Availability: ensuring that authorized users have access to information whenever they need it;
Privacy: guarantee the protection of customers, providers, candidates and employees personal data, regarding the fundamental right of each individual to have access and decide who should have access to their data.

Information Security Policy Scope Principles

All employees, trainees and service providers are bounded to not to transfer, disclose, divulge, use or discuss, directly or through an intermediary, any information and / or elements entrusted to them or that they have had knowledge in the exercise of the its activity, namely the organization, method and work processes, as well as represented brands, products, identification of customers and suppliers and any technical or financial details. According to ISP and for all legal purposes, especially for criminal and civil effects, they will have to maintain secrecy / confidentiality and / or professional secrecy, being expressly forbidden to disclose or use information from Passio Consulting clients in the course of their professional activity.

The ISP presents five (5) large areas, where Passio Consulting defines objectives and control mechanisms for each area:

1. **Human Resource Management**: Human Resource-related security management and includes periodic training and workshops.
2. **Technology and Systems Management:** security management related to logical assets (information system) and physical (computers, networks) and access management to these assets.
3. **Information and Communication Management:** security management related to access to information according to its classification and also how this communication is carried out in and out of Passio consulting.
4. **Incident Management:** management of security incidents and mechanisms to detect and respond to these situations.
5. **Privacy and Personal Data:** personal data protection management for those who related to Passio consulting, whether employees, customers, suppliers, candidates, service providers, ensuring compliance with legal regulations in force and the right of each individual in deciding who can access your information and what information can be accessed.

Information Security Policy Responsibilities, Maintenance and Communication

The ISP must be communicated to all employees, trainees and service providers of Passio Consulting, so that it is fulfilled inside and outside the company.

The responsibility concerning information security, must be communicated when employees, trainees or service providers are contracted. All employees, trainees and service providers should be guided on the Information Security Policy and the correct use of information assets in order to mitigate risks.

A Privacy and Confidentiality Clause is included in all Passio Consulting contracts as an essential condition for the information to be made available.

The Information Security Policy is top management responsibility, along with implementation control and evaluation.

The Information Security Policy must be periodically reviewed in order to ensure it remains adequate to Passio Consulting.