FONDO ACCION

INFORMATION SECURITY INTERNAL POLICIES AND PROCEDURES

FONDO ACCION
Tels: (+571) 2853862 Telefax: (571) 2454145
Carrera 7 Nº 32 – 33 piso 27
www.fondoaccion.org
Bogotá D.C. Colombia

FONDO PARA LA ACCIÓN AMBIENTAL Y LA NIÑEZ-FONDO ACCIÓN

INFORMATION SECURITY INTERNAL POLICIES AND PROCEDURES

CONTENTS **Page.**

FONDO ACCION
Tels: (+571) 2853862 Telefax: (571) 2454145
Carrera 7 Nº 32 – 33 piso 27
www.fondoaccion.org
Bogotá D.C. Colombia

Presentation

Fondo Acción is a non-profit Organization incorporated under the laws of Colombia. In accordance with Law 1581 of 2012 *"By which laws for the protection of Personal Data have been enacted"* and its regulations, the following Information Security Policy and internal procedures has been incorporated.

With the enactment of this Information Security Policy and internal Procedures, **Fondo Acción** formalizes its commitment with the responsible management process with the purpose of ensuring its integrity, confidentiality and availability, in accordance with the applicable data protection laws.

1. Information Security

Information security is defined as the protection, assurance and compliance with the nature of the information such as: confidentiality, integrity, availability, complying in any event, with the legal, regulatory and statutory standards of **Fondo Acción**.

2. Scope

This information security Policy and internal procedures, applies to all employees of **Fondo Acción** at all levels. It applies to all databases and personal information files held by **Fondo Acción** and which are within the general framework of Law 1581 of 2012 and its regulations.

3. Objectives

Protect, preserve and manage the information of **Fondo Acción,** as well as the technologies used for its processing, against internal or external threats, whether deliberate or accidental, to ensure the confidentiality, integrity, availability, legality, reliability of the information.

4. Responsibility

The Information Security Policy and Internal procedures of the Information is mandatory for all personnel of **Fondo Acción,** regardless of his/her contractual situation, the Area he/she is assigned to and the level of tasks he/she performs.

The Systems Area, with the support of the Legal Area of **Fondo Acción,** will be responsible for the review, update and approval of the text of this Policy.

The Systems Area will be responsible for promoting the implementation and compliance of this Policy, as well performing functions related to the security of the entity's information security.

The Systems Area shall follow the guidelines of this policy and shall comply with the information security requirements established by **Fondo Acción** for the operation, management, communication and maintenance of its information systems and technology resources.

The Legal Area shall notify all of the personnel contracted by **Fondo Acción** of all the obligations with respect to the compliance of the Information Security Policy and the changes therein. Additionally, it shall verify the compliance of this Policy in the management of all contracts with employees and third parties of **Fondo Acción** and advise the organization in al legal matters related to information security.

The personnel of **Fondo Acción** which uses the information and the technology platform for its processing, is responsible for knowing and complying with this Information Security Policy.

5. Information Security with respect to the Human Resource of Fondo Acción

Fondo Acción protects the information it collects in a secure database. In the storage of the information we have taken a series of measures to protect the information against unauthorized use, loss, unauthorized access, amendment or unauthorized disclosure. **Fondo Acción** uses firewalls, intrusion detection systems and tools to detect virus to protect the data.

In addition, the employees of **Fondo Acción** require as a condition for employment, the confidential handling of all the information held by **Fondo Acción**, and to maintain the confidentiality of said information. Also, they are assigned user names and passwords to access the applications and data storage units of **Fondo Acción**.

The management of users is the responsibility of the Systems Area, as well as new entries, application privileges and deleting users.

6. Physical and environmental Security

6.1 Access

The physical access to the offices of **Fondo Acción** is controlled; the wireless networks do not allow access to the local network; external personnel to the organization cannot connect to the LAN; if, for any reason, it becomes necessary, the Systems Manager will supervise this operation.

Another level of controlled access is the ICT room, which can only be accessed by the Systems Manager.

Remote access is not allowed from the outside in and, if this type of connection is necessary, the Systems Manager will also supervise this operation.

6.2 Hardware security

Fondo Acción provides the necessary infrastructure to operate safety with respect to level of electric fluid, own environment, unauthorized physical and virtual access. The structured cabling is completely supervised. The servers, which store the information and services, are maintained in a preventive and corrective manner at the hardware and software

level. Additionally, it has: a) fire detection and extinction of conflagrations systems, b) low risk of flooding, c) insurance for equipment that covers accidents, d) regulated electric systems backed up by uninterrupted power sources (UPS).

The individual equipment assigned to the personnel at **Fondo Acción** must be installed correctly and must be operated by personnel of the organization trained to operate them, also, with respect to the contents of this policy and the personal responsibilities in the use and the administration of the institutional information.

The media that stores security copies must be adequately preserved and protected in accordance with the standards established by the Systems Area for such purpose.

There is a policy for the creation and handling of security copies, which is part of the Quality Management System, entitled: DA-MA-06 Contingency Plan and SGC backup Policies.

7. Management of communications and operations

7.1 Report and investigation of security incidents

The personnel at **Fondo Acción** must report with diligence, promptness and responsibility to the Systems Area alleged security violations to the information.

7.2. Protection against malware, software and hacking.

At the very least, the individual work equipment of **Fondo Acción** must be protected by Antivirus, Spyware, Malware software with update capabilities. The station users are not authorized to disable this control nor install unauthorized or illegal software.

7.3 Exchange of Information with External Organizations.

All the institutional information must be managed in accordance with current laws regarding the matter (Law 1581 of 2012 and regulations)

7.4 Internet and email

The use of Internet and email services must ensure compliance with **Fondo Acción's** Ethic's Code and the responsible use of information technology resources.

7.5 Software Installation

All software installations performed in **Fondo Acción's** systems, must be approved by the Systems Area. The installation of software that violates intellectual property and copyright laws is not allowed.

8. Access Control

8.1 Access Categories

The access to institutional information technology resources should be restricted in accordance with the user profiles defined by the Systems Area, for such purpose **Fondo Acción** has the document DA-MA-07 USE OF SHARED SERVER SPACE AND FORMAT POLICY, which is part of the Quality Management System.

8.2 Password and User Name Control

In addition, the employees of **Fondo Acción** require as a condition for employment, the confidential handling of all the information for personal data handling held by **Fondo Acción,** and to maintain the confidentiality of said personal information. They are also required to use user names and passwords to access **Fondo Acción's** systems.

As a requirement for the termination of the contractual or employment relation of **Fondo Acción's** personnel, the Systems Area must cancel the user accounts assigned for the use of the information technology resources of the organization.

9. Acquisition, Development and Maintenance of Software Systems

To support its strategic and operational processes, **Fondo Acción** makes intensive use of Information Technologies and Communications. The software systems used may be purchased through third parties o developed by its own personnel.

10. Compliance

All use and monitoring of use of **Fondo Acción's** IT resources must comply with the laws and internal statutes as well as national laws in the matter.