Security Protocol

Information security is critically important to us. As stated in the Policy of ”La Strada” International Center, we will put all available effort into protecting the collected information from threats – whether internal or external, deliberate or accidental. We are guided in our activity by the following principles:

- Confidentiality - Prevention of unauthorized disclosure of information;
- Integrity - Preventing the unauthorized modification of information;
- Availability - Appropriate setting of access and security levels to prevent unauthorized access and maintaining the legal ones.

Our commitment to information security is demonstrated by implementing information security management procedures. The procedures include requirements and rules for the protection of all kinds of information, including personal data.

Security and data protection in the information system of the Hotline is carried out through the following measures:

1. General measures:

- Security and physical access to the means of displaying the information is ensured in order to prevent the information being seen by unauthorized persons (computer screens are not visible from the outside and cannot be seen by other employees of the organization; windows are covered with a matte film of protection or blinds).
- All the programs used in our computer systems comply with the current licensing requirements. The programs are installed by the computer system administrator.
- Antivirus software is installed to protect data from cyber-attacks, malware or identity theft.

2. The security of the physical environment and the information technologies used in the information processing process:

- Access to the office of the Hotline, where the personal data information systems are located is restricted. Only persons with a specific level of authorization or clearance are permitted on premises (analysts, the Hotline manager etc.).
- The access to the building through the main entrance is secured by a padlock and a card-chip system, that only authorized persons or their guests have access through. The door is always locked and there are visible ***”no entry”*** signs displayed.
- The perimeter of the building or the rooms where the means of information processing are located is physically intact, the external walls of the rooms are resistant, the entrances are equipped with locks and signage.

- The location of the information processing means corresponds to the regulations meant to ensure their security against unauthorized access, theft, fires, floods and other possible risks.
- The computers, servers and other access terminals are located in places with limited access to outsiders.
- Photo, video, audio and/or other means of data recording in the Hotline's office is prohibited unless it was previously discussed and authorized by the management.

3. User authentication and access control

- The identification and authentication of the users of the information systems of the Hotline and of the processes executed on behalf of these users is carried out.
- All users (analysts, the Hotline manager, the network administrator etc.) have a personal user ID, which corresponds to the user's access level.
- To confirm the user's ID, passwords, special physical means of access with memory or cards with microprocessors, biometric means of authentication, based on unique and individual characteristics of the person, are used.

New employees within the Hotline are trained in information security during their induction period. All staff must attend regular refresher training sessions to ensure that their knowledge and understanding remain up to date.

We have a separate Privacy Policy which explains the specific arrangements in place regarding the processing of personal data. This can be found on our website: www.siguronline.md.

We believe that complying with our up to date information security procedures is a shared responsibility that we all take very seriously.