Data Security Policy

Regulations on Data Security (Information Security) of Non-governmental Organization "Ukrainian Pet Association Worldwide”

1. General Terms and Scope of Regulation

1.1. Definition of Terms:

- Business Process shall be a structured sequence of actions to perform a certain type of activity at all stages of the activity operational lifetime, the purpose of which is to obtain a given result that is of value to the NGO.
- Threat shall mean a potential cause of an unwanted incident that could result in damage to a system or organization.
- Information Security shall mean protecting information from a wide range of threats to ensure business continuity, minimize business process risk, and maximize return of investments and business opportunities.
- Unauthorized Person, Object or Process shall mean a person, object or process that is not controlled by the NGO and/or does not satisfy the requirements specified.
- Authorized Object shall be an object that is controlled by the NGO and/or satisfies the requirements specified.
- NGO shall mean Non-governmental Organization "Ukrainian Pet Association Worldwide”

1.2. This Policy shall be mandatory for application by the authorized person, employees and members of the NGO

2. Purpose of the Policy

Data (information) is a resource that, like other important business resources, has a certain value for the NGO and, therefore, shall be appropriately protected.

The Purpose of the Policy shall be implementation of measures aimed at the NGO protection from possible material, reputational or other damage, which may be caused by accidental or intentional influence on the objects of protection.

This goal shall be achieved by ensuring the properties of the protected objects, such as availability, integrity and confidentiality.

The required level of availability, integrity and confidentiality shall be ensured by implementation of organizational and technical measures developed on the basis of an assessment of information security risks peculiar to the objects of protection.

3. Objects of Protection

3.1. Among the main objects covered by the information security of the NGO, the following types of resources shall be considered:

• information resources shall be information and data in any form, received, stored, processed, transmitted, declared, including knowledge of employees, partners of the NGO, databases and files, documentation, user manuals, training materials, descriptions of procedures, archived information, etc.;

• software shall be application program software, system software, service software and any other software, regardless of the form of acquisition (purchase, own development, free distribution), which is used by the NGO, employees and systems to work and interact with contractors and others internal and external systems;

• physical resources shall be employees, hardware resources (servers, workstations, firewalls, printers, copiers, telecommunications equipment, communication equipment, routers, PBXs, fax machines, modems, etc.), storage media (tapes, disks etc.), furniture, premises, production equipment, other technical means, etc.

• service resources shall be computing and communication services (Internet, e-mail, communication channels, etc.), other technical services (heating, lighting, energy saving, air conditioning, alarm and monitoring systems), all services related to receiving, providing, use, transfer and destruction of resources, all legal entities and natural persons, organizations, institutions (as well as their employees), the services of which are used by the NGO to receive, use, transfer and destroy resources.

3.2. For each resource, possible information security risks and ways to minimize them shall be determined, that is, the NGO shall use a risk-based approach that provides understanding, monitoring and reducing the risks of activities.
3.3. To ensure the required level of the NGO functioning, the following protection shall be provided:
- automated system of the NGO: a complex of hardware and software designed to automate the business processes of the NGO;
- premises in which elements of the automated system of the NGO are located;
- information which is processed and stored in the automated system of the NGO.

3.4. Personnel shall be a separate category that needs to be paid attention to in order to ensure information security of the NGO.

4. Policy Implementation Principles

4.1. To achieve its goals, the Organization intends to be guided by the following principles:
- legality: The Organization shall implement measures to ensure information security in accordance with applicable law and contractual obligations;
- involvement of the NGO senior management in the process of ensuring information security: the activity shall be initiated and controlled by the NGO senior management;
- economic expediency: The Organization shall seek to choose measures to ensure information security, taking into account the costs of their implementation, the likelihood of information security threats and the amount of possible losses from their implementation;
- completeness and consistency: information security shall be implemented at the legal, administrative, procedure, as well as software and hardware levels;
- personal liability: employees and management of the NGO, as well as representatives of a third party interacting with the Organization, shall be liable for compliance with information security requirements;
- minimum sufficiency: access to the information resources of the NGO shall be provided solely on a need-to-know basis and at the level of the minimum required authority;
- taking into account information security requirements in project activities: development and documentation of requirements to information security products shall be carried out at all stages of project implementation.
- integrity: characteristic of security, correctness and completeness of the NGO resources.
- confidentiality: characteristic of information not to become available and disclosed to unauthorized persons, objects or processes.
- availability: characteristic of accessibility and the ability to use the NGO resources at the request of the authorized object.
- observability: characteristic of a system (automated, access control, monitoring, etc.) to record the activities of identified users and processes. This shall primarily be applied to information with restricted access, which includes information constituting a trade secret, personal data and other confidential information.

5. Scope

5.1. The information security principles set out in the document shall be applied to all departments of the NGO from the scope of the information security management system, and shall be also applied to other organizations, institutions and individuals interacting with the NGO as suppliers or consumers of information resources of the NGO.
5.2. The NGO shall ensure compliance with all information security requirements that are in agreements with third parties regarding participation in international payment systems and funds transfer systems.

6. Supplementary Conditions

The NGO shall reserve the right to change the terms and conditions herein at any time.