



APPROVED
Executive Director
NGO «Technology of Progress»
Zadvornyy V.V.
April 8, 2025

Approved
By Order No. 2-D dated April 8, 2025

Approved
By the Decision of the Extraordinary General
Meeting No. 1-P dated April 8, 2025

POLICY ON THE DUTY OF CARE

Kyiv, 2025

1. Introduction

1.1 The activities of the NGO «Technology of Progress» (hereinafter referred to as the «Organization») are based on the values of proactivity and care, partnership and cooperation, responsibility and the rule of law.

1.2 The Organization adheres to the highest standards of integrity and professionalism, regardless of the environment in which it operates. The Organization requires its employees, officers, and members to always uphold the highest standards of ethical conduct. In order to enable and facilitate the fulfillment of these duties, the Organization commits to providing a work environment that encourages high standards of performance, professional and personal development, the achievement of organizational goals, and prioritizes the health and safety of its staff.

2. SCOPE OF APPLICATION

2.1 This Policy applies to all employees, staff members, officers, and members of the Organization (hereinafter referred to as the «Personnel»).

2.2 The provisions of this Policy may also apply to any party contributing to, implementing, executing, or otherwise participating in activities related to the Organization, including any form of funding or support from the Organization (grantees, suppliers, sub-grantees, beneficiaries, stakeholders, consultants, external contractors, engaged experts, volunteers, and other related entities), if their respective agreement (contract) stipulates the obligation to comply with this Policy (hereinafter referred to as the «Representatives»).

2.3 The implementation of this Policy is directly overseen by:

- The General meeting of the Organization;
- The Executive Director of the Organization.

3. PURPOSE

3.1 The purpose of this Policy is to provide Personnel and Representatives with a clear understanding of the procedures and practices employed by the Organization, as well as to ensure a healthy and safe working environment for the personnel.

3.2 The Policy also provides an overview of how the Organization assesses, monitors, and responds to security risks that may affect the personnel and the implementation of the Organization's projects.

4. TERMS USED

4.1 Activity related to the Organization: any activity that is funded, managed, or supported by the Organization, whether through its own resources or those of other entities; any activity that significantly affects or may affect the Organization's operations; or any activity conducted on behalf of the Organization or using the Organization's trademark or logo.

4.2 Duty of Care: a legal obligation requiring an individual to take reasonable measures to avoid causing harm or injury to themselves and/or another person for whom they are responsible.

4.3 Breach: a breach of the duty of care occurs when an individual acts unreasonably or fails to act where action could reasonably be expected, resulting in harm.

4.4 Reasonable Precaution: the level of caution and care for one's own safety and the safety of others that a prudent and rational person would exercise under the given circumstances. Failure to exercise reasonable precaution constitutes negligence.

4.5 Reasonable Person: (in the context of the definition of «Reasonable Precaution») another individual in the same situation would act in the same or similar manner.

4.6 Risk: a situation that exposes an individual to danger, harm, or loss.

4.7 Injury: means personal or bodily harm and includes:

- a) psychological or mental trauma;
- b) illness;
- c) aggravation, acceleration, or recurrence of an injury or illness.

4.8 Harm: refers to damage of any kind and includes:

- a) bodily injury or death;
- b) property damage;
- c) economic loss; and
- d) reputational damage or moral harm.

5. AREAS OF ACTIVITY AND SCOPE OF RESPONSIBILITY

5.1 Individuals directly involved in the implementation of this Policy are responsible for:

- Ensuring the physical safety and protection of the life and health of the Personnel while present in the workplace;
- Ensuring the information security of the Organization, including intellectual property;
- Ensuring the information security of the Organization's Personnel;
- Ensuring the preservation of the Organization's material assets;
- Ensuring the financial security of the Organization.

5.2 Representatives, under the conditions specified in Clause 2.2 of this Policy, and Personnel are responsible for:

- Ensuring compliance with this Policy and other related policies;
- Exercising reasonable caution while performing their duties and maintaining responsibility for their own health and safety, as well as that of others in the workplace;
- Actively contributing to the creation and maintenance of a safe environment through open communication, clear boundaries, complaint or disclosure management, accurate documentation, and reporting any risk or harm to the relevant authorities in accordance with applicable procedures;
- Anticipating foreseeable harm and risks to themselves and/or others and immediately reporting any hazardous conditions or behaviors observed in the workplace in accordance with the procedures established for each specific situation that may potentially result in harm;
- In the event of identifying foreseeable harm or risk, taking preventive and risk control measures in coordination with their immediate supervisor (where practically possible) and in accordance with established procedures;
- Exercising the level of caution expected of a reasonable person.

6. ORGANIZATION'S DUTIES IN THE FIELD OF SAFETY AND RIGHTS PROTECTION

6.1 The Organization prioritizes the safety and health of its Personnel, taking all possible measures to ensure their protection. The Organization guarantees the opportunity to attend safety trainings, including procedures in high-risk situations, first aid, and other measures, considering the Organization's financial capabilities.

6.2 Every person among the Personnel or Representatives of the Organization is responsible for familiarizing themselves with the safety plans and instructions, including after any updates.

6.3 Every person among the Personnel or Representatives must understand their responsibility for themselves and the team, as well as the risks for themselves, the team, and the tasks they perform.

6.4 Every person among the Personnel or Representatives is obliged to immediately report safety-related incidents to the Executive Director of the Organization. While at the workplace, these persons report safety threats in person. When working remotely, they should report by phone or email.

6.5 The Organization takes all measures regarding Personnel or Representatives during business trips (especially to remote areas or high-risk zones) by:

- Assessing the situation (based on official information from government authorities and coordinating international organizations);
- Developing routes and travel schedules;
- Informing about movements;
- Providing necessary informational preparation;
- Conducting briefings on emergency reporting procedures;
- Conducting briefings including standard instructions for behavior in specific regions (e.g., at checkpoints, restricted or prohibited zones) or under certain conditions.

6.6 The Organization cares for the safety of its Personnel and Representatives, therefore, when selecting projects, priority is given to assessing risks to the health and safety of employees. The Organization tries not to involve these persons in gray zones or combat zones and informs them about the location of the nearest bomb shelter and the necessity of responding to alerts about shelling threats.

6.7 To ensure safety, the Organization's office must be equipped with a fire extinguisher, first aid kit, personal protective equipment, and an action plan (including information about the nearest bomb shelter) in case of missile threats.

6.8 Before the start of each project, the Organization conducts a risk assessment to identify threats and vulnerabilities, assess their likelihood and impact, and determine mitigation options. An introductory meeting is held where team members are informed about the project progress, potential risks, and methods/tools for minimizing them. Work chat groups are created for operational information sharing. Steps include:

- Assessing potential threats to employees at all project stages;
- Analyzing risks and their likelihood;
- Determining possible risk reduction steps;
- Making decisions based on the assessment;
- Ongoing monitoring of threats during project implementation.

6.9 The Organization, Personnel, and Representatives are obliged to:

- Take all reasonable measures to ensure that the working environment, materials, actions, and activities are free from discrimination, harassment, bullying, victimization, intimidation, or other inappropriate conduct;
- Promote the implementation of inclusive practices in the Organization's activities;
- Conduct trainings on nondiscrimination and equality and implement awareness-raising projects;
- Ensure an effective complaint submission and review procedure based on principles of fairness.

6.10 The Organization continuously monitors the national and international legal framework on nondiscrimination and equality.

6.11 The Organization's corporate email for suggestions and complaints: info.technology.progress@gmail.com

6.12 For the purposes of this section, the following definitions also apply:

Consent — giving permission or agreeing to something with full understanding and without coercion.

False or malicious report — inaccurate or misleading reporting made negligently, knowingly, or intentionally to gain improper advantage or cause harm to a person or entity.

Sexual violence — actual physical sexual acts or threats thereof, committed with force or under unequal or coercive conditions.

Sexual exploitation — any actual abuse or attempted abuse of a vulnerable position, power, or trust for sexual purposes, including but not limited to threats or obtaining financial, social, or political gain through sexual exploitation of another person.

Sexual harassment — any unwanted sexual advances, requests for sexual favors, or other verbal, nonverbal, or physical conduct of a sexual nature that interferes with work, is a condition of employment, or creates an intimidating, hostile, or offensive environment in connection with Organization-related activities. Sexual harassment can occur between persons of different or the same sex or gender and can be initiated by any person regardless of gender or sex.

Victim — a person who has experienced or is experiencing sexual exploitation, violence, or harassment.

6.13 Personnel and Representatives mentioned in Section 2 of this Policy must adhere to the following principles:

- Sexual exploitation and sexual violence are gross disciplinary offenses and grounds for termination of employment or civil-law contracts;
- It is prohibited to exchange money, work, goods, or services for sex, including sexual services or other forms of humiliating, offensive, or exploitative behavior;
- Personnel and Representatives must not engage with any third party who condones, encourages, participates in, or is involved in sexual exploitation and abuse (hereinafter – the «SEA»);

- If Personnel or a Representative has concerns or suspicions regarding sexual violence or exploitation by a colleague, regardless of whether they work in the same organization, they must report it using established reporting mechanisms;
- Personnel and Representatives are required to create and maintain an environment that prevents sexual exploitation and abuse. Managers at all levels are responsible for supporting and developing systems that promote such an environment.

6.14 The Organization commits to creating and maintaining a work environment free from sexual harassment and violence, respecting the dignity of all people, fostering an atmosphere that allows them to fully realize their potential and achieve the best results. The Organization recognizes the need to actively combat any silent or explicit manifestations of sexual harassment or sexual violence and commits to improving understanding of the issue among Personnel and Representatives to prevent its occurrence, as well as to creating a culture of support that encourages reporting incidents and ensures they are properly addressed.

6.15 To establish and maintain a SEA prevention and response system, the Organization may appoint the SEA dedicated expert.

6.16 The SEA dedicated expert provides Personnel and Representatives with informational materials, organizes and conducts SEA trainings, and serves as a contact person for reporting SEA cases. The SEA dedicated expert must carefully report suspicions of SEA independently and objectively by conducting investigations free from control or influence by any individual or legal entity, with strict adherence to principles of fairness and due process.

6.17 Individuals reporting actual or suspected cases of SEA must do so in good faith and provide any available information or evidence supporting a reasonable belief that SEA may have occurred. Before reporting, they are not required to assess or determine if the report meets any threshold of severity. Persons reporting suspected SEA are not required to prove the suspicion or meet evidentiary standards.

6.18 Any Personnel or Representative who has become a victim of SEA related to the Organization's activities and about whom a report has been made may request temporary medical and psychological assistance or other support services from the Organization.

6.19 Acts of retaliation against an actual or suspected SEA victim committed by a Personnel member or Representative of the Organization are considered misconduct or contract violation and require disciplinary or other appropriate measures.

6.20 The working regime of Personnel, including days off, business trips, and vacations, is determined in accordance with current Ukrainian legislation and internal labor regulations. The Organization independently sets the work schedule according to the directions of work and project specifics.

6.21 The Organization prioritizes the life and health of Personnel. It ensures Personnel can contact their immediate supervisor to change work regime, including temporarily changing work nature, location (including remote work), obtaining days off, or special leave to avoid professional burnout and promote effective duty performance.

6.22 Personnel must report any circumstances, including force majeure, affecting their employment in relation to the Organization's activities by notifying their immediate supervisor, except when impossible.

6.23 The Organization promotes continuous professional development of Personnel, including intellectual, professional, creative, and sports qualities, individually and collectively. The

Organization takes all possible measures to develop its potential considering its financial capabilities.

6.24 The Organization defines the need to maintain proper protection of information, software, and technical resources, ensuring their integrity, confidentiality, legality, availability, and monitoring. Information security includes information literacy, delegation of authority, access and transmission rules, confidentiality, respect for intellectual property rights, and preservation of archival copies.

6.25 Information security rules apply to Personnel and Representatives of the Organization.

6.26 The Organization keeps records of information, software, and technical resources owned by the Organization and defines procedures for creating, accessing (including subject circles), storing, modifying, and destroying information.

6.27 The Organization defines the need for proper storage, processing, and transfer of personal data of Personnel and Representatives.

6.28 The Organization defines the need for proper storage, processing, and transfer of donors' personal data with notification of such actions.

6.29 The Organization defines procedures to ensure information security in cooperation with private information providers, donors, government and local authorities, international and non-governmental organizations, media, and other individuals and legal entities.

6.30 The Organization ensures compliance with intellectual property rights, copyright, and related rights concerning and related to it, defining responsibility according to current legislation.

6.31 An emergency situation is understood as a danger of natural, technological, socio-political, or military nature, war, anti-terrorist operation, or other heightened danger measures of national, regional, or local character that may affect the Organization's goals, and the safety of Personnel and Representatives.

6.32 According to the emergency situation assessment, the Organization takes all measures to preserve the Organization's assets and protect the life, health, rights, and interests of Personnel and Representatives.

6.33 In case of a situation posing a potential threat to the life and health of Personnel while in the office, a remote work mechanism has been developed. The Organization provides equipment and algorithms enabling continuation of work without loss of quality remotely. Every Personnel member or Representative can stay in a safe place and perform all tasks. Access to work documents is provided via the Organization's Google Drive. Coordination is done via phone or online communication tools: Zoom, WhatsApp, Gmail, Asana, etc. Regular meetings and work control occur during remote work.

7. VIOLATION OF THE POLICY

7.1 The duty of care is considered breached if a Personnel member or Representative:

- Does not act as a reasonable person would in their position under the same circumstances;
- Their actions or inactions may cause or have caused harm to a person with whom they interact and toward whom they owe a duty of care, including physical, emotional injury, or financial damage.

7.2 The Organization takes its duty of care extremely seriously. Personnel who violate this Policy or any related policies or procedures will be subject to disciplinary action, and in the case of a serious violation, employment or other contractual (civil-law) relations with the person in

question must be terminated. The Organization reserves the right to terminate contractual relations with a Representative in case of violation of this Policy and its prescribed procedures.

8. ASSESSMENT OF VIOLATION INCIDENTS

8.1 Cases of breach of the duty of care are assessed by their severity using the following criteria:

- Low – affects a local environment and can be remedied through short-term measures, with no long-term consequences.
- Moderate – has a broader impact than the local environment, with protective measures easily accessible but requiring a longer time and/or involvement of several persons. Long-term consequences are possible but manageable. May require notification of regulatory authorities.
- High – the case has long-term consequences of negligence, may require financial or legal compensation, may include data breaches, may lead to short-term reputational loss, and requires notification of regulatory authorities.
- Extremely High – the case has serious consequences of negligence, requires financial compensation, involves prolonged litigation, may include significant data breaches, requires notification of regulatory authorities, and may cause long-term reputational damage.

8.2 The Organization complies with all reporting requirements for duty of care breaches. Incident reporting is conducted at the workplace and within work processes to minimize risks to the safety of all parties.

9. REPORTING AN INCIDENT

9.1 All cases of breaches of the duty of care must be reported to the Executive Director of the Organization.

10. FINAL PROVISIONS

10.1 This Policy comes into effect from the date of its approval by the Executive Director of the Organization.