ENERGO-PRO Group

Security Policy

2026

ENERGO-PRO

SECURITY POLICY (THE "POLICY")

1. Introduction

The core business of ENERGO-PRO a.s. ("ENERGO-PRO") and its subsidiaries (collectively "the Group") is renewable energy generation. The Group's additional activities include electricity distribution, supply and trading.

ENERGO-PRO is committed to protecting the security of the workforce, our value chain, visitors, and the communities impacted by our operations. ENERGO-PRO upholds the principles in the United Nation's Universal Declaration of Human Rights, the UN Guiding Principles on Business and Human Rights, the Voluntary Principles on Security and Human Rights (VPSHR) and the declaration of the International Labour Organization on Fundamental Principles and Rights at Work.

This Policy establishes the Group-level standard for security management across ENERGO-PRO operations and projects and sets out the requirements for identifying, preventing and managing security risks in a manner consistent with applicable laws, Good International Industry Practice (GIIP), our Group Code of Conduct, the Group's Human Rights Policy and other applicable ENERGO-PRO policies. Country-level procedures, plans and controls may define more detailed requirements based on local legal, operational and security conditions, provided that they remain aligned with this Group Policy. The requirements set out in this Policy are informed by ENERGO-PRO's salient human rights risks related to security, including the treatment of workers and communities, the conduct of security personnel, and the management of conflict and use of force.

2. Objectives.

The objectives of this policy are:

- To provide a secure working environment for all employees, value chain (contractors, sub-contractors and others) and visitors.
- To maintain and protect the security and integrity of operations, facilities and assets.
- To establish and maintain a relationship based on trust, mutual respect and integrity with the communities, local authorities and other stakeholders.
- To provide direction and build leadership, management and employee accountability.
- To respect and demonstrate Good International Industry Practice regarding human rights and security.

3. Governance

ENERGO-PRO's Group and Subsidiary Board of Directors are accountable for ensuring the implementation of this policy. Senior management is responsible for ensuring that the Policy is integrated into relevant business processes and operations.

4. Scope

The Policy applies to all employees and our Value Chain.

This Policy applies to ENERGO-PRO, ENERGO-PRO's subsidiaries operating in Bulgaria and Georgia and the subsidiary Murat Nehri Elektrik Üretim A.Ş. operating in Türkiye.

It also applies to all other subsidiaries of ENERGO-PRO, which may however request the Group Board of Directors to approve an opt-out from specific provisions of this Policy. The Group Board of Directors may approve such a request where it is satisfied that the opt-out is based on

objective and commercially reasonable grounds and, further, is consistent with local law, the Group Code of Conduct and binding financing commitments. Approved opt-outs will be documented and shared with the Group ESG Department.

We expect those working with and for us to uphold equivalent standards and may seek to assess alignment with these principles as part of our business processes.

5. Requirements

ENERGO-PRO recognizes the need to nurture a culture of security awareness and discipline, when working in remote or complex environments. The specific requirements of this policy are intended to establish a Group-level minimum standard and shall be applied, as relevant, to the legal, operational and security context of each country, office, project or operation.

1. Security Management

   Business unit(s) Board of Directors is responsible for ensuring that all offices and operations/projects are secure and that suitably qualified staff have been assigned to manage security. All construction/operation sites are required to have security measures and controls, including, as appropriate, construction/operations security risk assessments, and security incident reporting and management. Depending on the level of threat, assets located in environments which pose a security risk will also have in place Security Management Plans[1]. The Business unit's Board of Directors is responsible for assessing security materiality by evaluating the relevant threats and risks and accordingly determining the required level of security measures.

   The following considerations will be included in security management:

   I. Asset Classification for high security risk Business unit(s): Prior to any risk assessment, all project assets must be identified and categorized into four primary categories: Human (personnel and contractors), Physical (infrastructure and equipment), Information (intellectual property and data), and Reputational (brand integrity). Each category shall be assigned a criticality level to prioritize protection measures and resource allocation.

   II. Security Risk assessments: All Business unit(s) shall assess security risks, the robustness of the risk assessment will be dependent on the security materiality of the Business unit. The assessments will be conducted to identify the existing and predictable security risks associated with the project/operations and will include controls and mitigation measures to manage the risks. Sufficient financial and human resources must be allocated to implement the established controls, as well as to ensure their maintenance and monitoring.

   The assessment shall consider international, legal, and company requirements. Risk assessments will be reviewed according to level of threat or after a significant security event or change in operations. The frequency of risk assessments will be guided by (i) historical; (ii) political; (iii) socio-economic; (iv) ethnic issues; (v) religious considerations; (vi) presence or perceived presence of terrorist groups or extremists; (vii) opportunistic criminal activity; (viii) legal and compliance; (ix) location; and (x) significant community conflict.

[1] Guidance regarding security management is available from *"Good Practice Handbook: Use of Security Forces: Assessing and Managing Risks and Impacts".* 2017 IFC website.

High-level, ad-hoc country level security risks may be assessed from time to time by the Group's Board of Directors in collaboration with the Business unit(s).

Risk assessments will consider the following threats:
Physical security threats:

- ✓ Armed attack (terrorist or criminal)
- ✓ Kidnapping, ransom and extortion
- ✓ Theft and vandalism
- ✓ National or local civil unrest
- ✓ Host country Government instability or collapse
- ✓ Operational and environmental threats
- ✓ Transportation-related threats
- ✓ Accommodation-related exposures
- ✓ Geographic and climatic events
- ✓ Remoteness and limited access to emergency support
- ✓ Socio-economic tensions
- ✓ Ethnic or religious conflicts
- ✓ Community conflicts or excessive grievances
- ✓ Presence or perceived presence of terrorist or extremist groups
- ✓ Socio-political and community-related threats

Non-physical threats:

- ✓ Intimidation or coercion
- ✓ Threat by employees, including union members
- ✓ Economic coercion, including blackmail.
- ✓ Reputational or brand damage
- ✓ Information and technological threats
- ✓ IT disruption and operational downtime
- ✓ Cybersecurity risks affecting operations, infrastructure and personal data
- ✓ Cultural misunderstandings and local sensitivities

III. Security Management Plans: Business unit(s) located in high-risk security environments shall have in place security management plans. These plans will be tailored to the requirements of the project/operations and will be fit for purpose. The plans will explain how each project/operations will provide security and mitigate the associated risks. It will consider the complexities of that site including an appreciation for cultural, geographic and political influences. The Security Management Plan will explicitly mention that the use of force shall be proportional, lawful and strictly limited to situations where it is necessary to protect life or prevent serious harm.

Roles and responsibilities must be defined to address the identified risk levels, ensuring they are aligned with the level and complexity of the risks and applicable to the operation.

The security management plan will include a section on incident management and reporting. This section will outline a consistent approach for identifying, reporting, assessing, managing and responding to security incidents. It will also define the roles and responsibilities for incident management and reporting.

IV. Business Continuity Plan (BCP): High-risk Business unit(s) will prepare a BCP tailored to the Business unit's specific threat environment. These plans shall set out clear protocols for immediate response to materialised threats (e.g. armed attacks, kidnappings, or IT breaches) and define the recovery steps to ensure the resilience of operations with minimal downtime.

V. Emergency and Evacuation Planning: Security emergencies will be included in the individual asset Emergency Preparedness and Response Plan. Furthermore, high-risk Business unit(s) will maintain a Security Incident Response Plan (SIRP) and evacuation procedures including evacuation routes designed to ensure a coordinated and effective response to security incidents.

VI. Continuous Review & Improvement: Security plans and controls shall be monitored regularly and updated after any significant incident. A post-event debriefing process will identify gaps to ensure mitigation measures remain adaptive, proactive, and fit for purpose.

2. Security Contractors Due Diligence

Prior to engagement of security contractors, ENERGO-PRO in country offices will undertake a due diligence of the potential security contractor to determine their human rights track record, relevant qualifications and compliance with applicable legal requirements. A sample survey from the Human Rights Compliance Assessment (HRCA) is available upon request from the head office to conduct the due diligence. Security contractors are required to provide Human Rights awareness to all their staff, including training on appropriate conduct towards workers, communities and other stakeholders, as relevant to their role. In absence of this training, ENERGO-PRO country offices will provide this training.

3. Communities and Local Authorities

While developing and implementing site security plans there must be an awareness of community impacts. Security staff must work closely with the relevant social teams to minimise security negative impacts on local communities and to support appropriate communication and engagement, as relevant.

ENERGO-PRO recognizes the importance of establishing good working relationships with communities and local authorities. All sites with security personnel will establish appropriate processes for the management of community-related security issues, as relevant to the site context.

4. Human Rights

ENERGO-PRO has developed a Human Rights Policy that provides principles about our human rights expectations. The Human Rights Policy includes human rights risks related to security and conflict.

ENERGO-PRO shall ensure that employees, contractors and security personnel receive appropriate human rights awareness training.

5. Responsibility

- Senior management, including site managers are ultimately responsible for security.
- Senior management shall demonstrate commitment by ensuring that adequate financial and human resources are available to implement and maintain a secure environment.
- All security incidents and community grievances related to security shall be communicated immediately to senior management, including investigations reports and relevant control measures.

6. Communication

This policy is communicated at least once a year to all employee and value chain through multiple channels including onboarding programs, training sessions, our corporate website, email and SMS updates, office posters, contractor agreements, and other communication tools.

In addition, every Business unit is required to demonstrate how they integrate and comply with this policy including security contractor due diligence, training, and the communication of these expectations throughout our value chain.

7. Distribution

This document is available on the company website, incorporated in selected standard terms and conditions of business, and may be reviewed regularly based on feedback from our stakeholders and in response to regulatory changes.

8. Entry into Force

This version of the Policy enters into force and is effective on and from May 2026.