

**ENERGO-PRO Group**

---

# **Security Policy**

**2021**



**ENERGO-PRO**

## **SECURITY POLICY (THE “POLICY”)**

### **1. Introduction**

Our core business is the hydropower sector. We operate hydropower plants in Central and Eastern Europe, the Black Sea and the Caucasus. We are also engaged in the electricity distribution and power trading, operating large-scale distribution grids in Bulgaria and Georgia with more than 2.3 million grid customers.

Our company was established in 1994 in the Czech town of Svitavy, participating in the modernization and rehabilitation of hydropower energy in Central and Eastern Europe in the period of economic transition. The total installed capacity of our power plants is 1,243 MW, while the annual power generation is more than 3.8 TWh.

One part of the multinational group ENERGO-PRO, headquartered in Prague, is the Slovenian manufacturer of water turbines, Litostroj Power d.o.o., with projects delivered to more than 60 countries worldwide. Its subsidiary, Litostroj Engineering a.s., registered in the Czech Republic (formerly known as ČKD Blansko Engineering, a.s.), focuses on research, design and engineering works. Litostroj Group also supplies equipment for hydropower plants, including pumped-storage HPP and pumping stations.

ENERGO-PRO is committed to protecting the security of the workforce, contractors, 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. ENERGO-PRO requires all employees, visitors, contractors and sub-contractors to abide by this Policy.

### **2. Objectives.**

The objectives of this policy are:

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

### **3. The Requirements**

ENERGO-PRO recognizes the need to nurture a culture of security awareness and discipline, in particular when working in remote or complex environments. The specific requirements of this policy are:

#### **I. Security Management**

In country Senior Management 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

construction/operations Security Management Plans<sup>1</sup>, security risk assessments, security incident reporting and management and evacuation plan(s). Depending on the level of threat, offices located in environments which pose a security risk will also have in place Security Management Plans. The following considerations will be included in security management:

- Threat evaluation and risk assessment and management: A risk assessment is the starting point prior to developing any security management plan. The risk assessment will identify the existing and predictable security risks associated with the project/operations. Each project/operations must conduct a baseline security risk assessment, involving relevant stakeholders and including suitably trained security staff/consultants. It shall consider international, legal and company requirements. Risk assessments will be reviewed annually or after a significant security event or change in operations. The frequency of risk assessment 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.
- Risk assessments will consider the following threats:
  - Physical threats:
    - ✓ Armed attack (Terrorist or criminal)
    - ✓ Kidnapping, ransom and extortion
    - ✓ Host country Government collapse
    - ✓ National/Local Civil unrest
    - ✓ Theft
    - ✓ Transportation
    - ✓ Accommodation related exposures
    - ✓ Geographic/Climatic events
    - ✓ Remoteness
  - Non-Physical threats:
    - ✓ Intimidation or coercion
    - ✓ Economic coercion, including blackmail.
    - ✓ Reputational or brand damage
    - ✓ IT disruption and operational downtime
    - ✓ Cultural differences.
- National and local security capabilities. Assessments of security partners should be done to understand future security support. This can include National, regional and local government security forces, law enforcement, military, national, regional and local government, private security companies, embassies and consulates, Non-Governmental Organizations or associations, and local community leaders.
- Controls and Mitigation: Once threats have been identified, existing controls will be identified, implemented and monitored.
- Security Management Plans: All 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.

---

<sup>1</sup> Guidance regarding security management is available from “*Good Practice Handbook: Use of Security Forces: Assessing and Managing Risks and Impacts*”. 2017 IFC website.

II. Security Contractors

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. 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.

III. 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 negative impacts on local communities.

We cannot undermine the importance of establishing good working relationships with communities and local authorities. All sites will establish management of community-based security relations.

IV. Human Rights

ENERGO-PRO has developed a Human Rights Policy that provides details about our expectations regarding Human Rights. One of the focal areas of the Human Rights Policy is Security and conflict which states:

*“We provide awareness to our security contractors regarding human rights and appropriate behaviour with our partners and stakeholders. We undertake due diligence of our security contractors prior to contract award. We encourage communication, peaceful conflict resolution, and consensus building in our dealings with partners and stakeholders. We enforce strict controls on the use of force and limit the use of firearms on our sites as far as possible”.*

V. Responsibility

- Senior management, including site managers are ultimately responsible for security.
- Senior management shall demonstrate commitment by ensuring 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 control measures.

**4. Distribution**

This document is available on the company website, incorporated in selected standard terms and conditions of business, and may be reviewed by company executives, management, employees, contractors and subcontractors. This policy will be reviewed regularly and updated if necessary to meet the requirements of partners and stakeholders.

**5. Entry into Force**

This version of the Policy enters into force and is effective on and from July 15, 2021.