Translation from Lithuanian

DVAS
2023-03-28 No. *DVSta-0101-9V2*

APPROVED
by the Decision of the Board of the State Enterprise Ignalina Nuclear Power Plant, Minutes No 2023-3/VPP-5(1.160E of 28 March 2023

NUCLEAR SECURITY POLICY OF THE STATE ENTERPRISE IGNALINA NUCLEAR POWER PLANT

The nuclear security policy of the State Enterprise Ignalina Nuclear Power Plant (hereinafter referred to as the enterprise, the INPP) has been developed in accordance with the Nuclear Safety Requirements BSR-1.6.1-2019 "Physical security of nuclear facilities, nuclear facilities site, nuclear material and nuclear fuel cycle material" approved by the Head of the State Nuclear Power Safety Inspectorate on 4 April 2012 by the order No 22.3-37 (the updated version approved by the Head of the State Nuclear Power Safety Inspectorate on 5 November 2019 by the order No 22.3-271), and the requirements of the Management System Manual of the State Enterprise Ignalina Nuclear Power Plant, DVSta-0108-4.

The objective of the INPP nuclear security policy (hereinafter referred to as the policy) is to define the obligations of the INPP management in ensuring the INPP physical security, cyber security, and the basic principles of physical security and safety culture to be followed in ensuring the physical security of the INPP nuclear facilities, nuclear facility sites, nuclear material and/or nuclear fuel cycle material.

This policy replaces the nuclear security policy of the State Enterprise Ignalina Nuclear Power Plant, DVSta-0101-9V1.

The INPP nuclear security objectives:

1. The adequate protection of the nuclear facility, nuclear material and/or nuclear fuel cycle material against their unlawful possession or seizure is guaranteed.

2. The protection against unauthorised access by outside persons to the protected areas of the nuclear facility is ensured.

3. The nuclear facility, nuclear material and/or nuclear fuel cycle material is protected from actions that would directly or indirectly create a risk to human health and safety due to ionising radiation, as well as the disruption of the normal operation of nuclear facilities is prevented.

4. The prevention of the unlawful possession or seizure of the nuclear facility, nuclear material and/or nuclear fuel cycle material, as well as actions that would directly or indirectly create a risk to human health and safety due to ionising radiation, and the disruption of the normal operation of nuclear facilities is ensured.

5. Timely identification of cyber incidents, prevention of their occurrence and spread, management of the consequences of cyber incidents, and secure access to the enterprise's information infrastructure.

6. The security and protection of classified information held and prepared by the enterprise against its unlawful possession, loss, damage or disclosure, the management of classified information, the security of classified transactions organised by the enterprise and the organisation of the reliability assurance of the personnel working in the enterprise are ensured.

Definitions used in this policy:

1. **Physical security system employee** means a person whose main duties are to ensure the physical security of the nuclear facility, its site, nuclear and/or nuclear fuel cycle material (physical security system employees are the employees of the Physical Security Division and the officials of Visaginas Division of the Public Security Service under the Ministry of the Interior).

2. **Nuclear security** means any unlawful act (such as sabotage, terrorist act, illegal intrusion, theft, illegal disposition, cyber incident, event, or other act related to the foreseeable threat identified by VATESI), directed against the nuclear facilities, nuclear and/or other radioactive material and objects in which such material is stored or used, and the prevention, detection, and response to such acts.

To ensure nuclear security at the INPP nuclear facilities:

1. INPP Physical Security Division shall carry out:

1.1. organisation of physical security,

1.2. physical protection of buildings and premises located in the inner and especially important areas,

1.3. cyber security,

1.4. protection of classified information,

1.5. maintenance of physical security systems,

1.6. organisation of the reliability of personnel,

1.7. accounting and control of fissile material and sources of ionising radiation.

2. Visaginas Division of the Public Security Service under the Ministry of the Interior of the Republic of Lithuania (hereinafter referred to as PSS) shall carry out:

2.1. control of the restricted access area,

2.2. physical protection of buildings and premises located in protected area,

2.3. response to illegal actions.

The importance of nuclear security does not decrease during the decommissioning phase of the INPP, as new nuclear facilities are being built for the storage of nuclear fuel and other nuclear material and/or nuclear fuel cycle material.

The INPP management, recognising the importance of nuclear security, takes responsibility for the activities of the enterprise in the field of the INPP's nuclear security and undertakes:

1. To improve continuously physical security in all aspects of the decommissioning process.

2. To allocate the necessary resources to implement the established nuclear security objectives and targets.

3. To comply with all nuclear security legal requirements applicable to the enterprise. Recognising that only established procedures and their strict adherence can ensure physical security, the INPP undertakes to immediately incorporate the provisions of the nuclear security requirements of the legal acts of the Republic of Lithuania into the normative technical documents applicable at the INPP and regulating physical security.

4. To ensure a flexible and balanced physical security system of the INPP, designed to meet the specific anticipated threat posed to the enterprise as defined by the State Nuclear Power Safety Inspectorate (hereinafter referred to as VATESI). To review and evaluate the physical security system as the anticipated threat changes. To take organisational and technical measures to eliminate weaknesses or non-compliances as soon as they are identified.

5. To implement Principle 5 of the International Atomic Energy Agency's (hereinafter referred to as the IAEA) document "Fundamental Safety Principles" No SF-1 – Optimisation of protection to provide the highest level of safety that can reasonably be achieved.

6. To perform analysis of the division of the INPP nuclear facilities into protection areas and to prepare Physical Security Assurance Plans.

7. To perform control of additional protection areas within the protected area of the nuclear facility.

8. To develop the enterprise's cyber security policy and to organise its implementation.

9. To monitor the cyber space of the enterprise's information infrastructure, to analyse the cyber security status of the enterprise's information infrastructure, to evaluate arising cyber threats, risks, and weaknesses.

10. To develop a cyber security culture within the enterprise.

11. To strengthen the enterprise's cyber defence by introducing advanced organisational and technical cyber security measures.

12. To ensure that all personnel working at nuclear facilities and on the nuclear facility site, as well as employees of contractor organisations, recognise the importance of nuclear security and the culture of safety and security, and consciously comply with the requirements.

13. To maintain accounting and control of nuclear material, small quantities of nuclear material and sources of ionising radiation.

14. To prepare reports on nuclear material accounting and inventories and submit them to the European Atomic Energy Community (hereinafter referred to as EURATOM) and VATESI.

15. To ensure assistance and participation in inspections carried out by the IAEA, EURATOM and VATESI in the field of nuclear material control, in compliance with international warranty obligations.

The enterprise, taking responsibility for the results of its activities and to ensure the physical security, chooses optimal measures in its activities and involves highly qualified employees in the field of physical security system.

The management of the enterprise shall ensure that the INPP nuclear security policy is accessible, known, and understandable to every employee of the enterprise.

This policy is evaluated each year as part of the analysis of the effectiveness and efficiency of the INPP management system.

The INPP nuclear security policy may be amended or recognised as expired by the decision of the INPP Board.

_____

Prepared by
The Head of the Physical Security Division
Marius Pernavas, tel. 29856

E. B., 1, 2023-04-17

Translated by Ema Banevičienė,
Translator of Document Management and Administration Division of SE Ignalina NPP,
2023-04-17