Translation from Lithuanian language

DVS
08-04-2020 No. *DVSta-0101-9V1*

APPROVED
by the order of the Director General
of the State Enterprise
Ignalina Nuclear Power Plant
No. ĮsTa-117 of 8 April 2020

PHYSICAL SECURITY POLICY OF THE STATE ENTERPRISE IGNALINA NUCLEAR POWER PLANT

The physical security policy of the State Enterprise Ignalina Nuclear Power Plant (hereinafter – the enterprise, INPP) has been developed according to the Nuclear Safety Requirements BSR-1.6.1-2012 "Physical Security of Nuclear Facilities, Nuclear Facilities Site, Nuclear Material and Nuclear Fuel Cycle Material", approved by the order of the Head of the State Nuclear Power Safety Inspectorate, No. 22.3-37 of 4 April 2012 (the updated version approved by the order of the Head of the State Nuclear Power Safety Inspectorate, No. 22.3-271 of 5 November 2019), as well as the requirements, defined by the Management System Manual of the State Enterprise Ignalina Nuclear Power Plant, DVSta-0108-4.

The objective of the INPP physical security policy is to establish the responsibilities of the INPP management to ensure physical security, cybernetic security and the basic principles of physical security and safety culture, which should be observed while ensuring the physical security of INPP nuclear facilities, nuclear facilities site, nuclear material and (or) nuclear fuel cycle material, and sources of ionizing radiation.

This policy replaces the physical security policy of the State Enterprise Ignalina Nuclear Power Plant, DVSta-0108-1V3.

The objectives of the INPP physical security are as follows:

1. Guaranteed adequate protection of the nuclear facility, nuclear material and (or) nuclear fuel cycle material and sources of ionizing radiation from their illegal occupancy or capture.

2. Ensured protection against unauthorized access by extraneous persons to the protected areas of the nuclear facility.

3. Secured protection of the nuclear facility, nuclear material and (or) material of the nuclear fuel cycle and sources of ionizing radiation from actions that directly or indirectly would cause the threat to human health and safety due to ionizing radiation, while also eliminating the cessation of the normal operation of the nuclear facility.

4. Secured prevention of illegal occupancy or capture of the nuclear facility, nuclear material and (or) of the nuclear fuel cycle material and ionizing radiation sources, as well as actions that directly or indirectly would cause the threat to human health and safety due to ionizing radiation and may interfere with the normal operation of the nuclear facility.

5. Timely identification of cybernetic incidents, preventing their occurrence and spreading, managing the consequences of cybernetic incidents, providing the possibility for the safe use of the enterprise's information infrastructure.

The importance of physical security during the decommissioning phase of the INPP does not decrease since new nuclear facilities are being built where spent nuclear fuel and other nuclear material and (or) nuclear fuel cycle material and ionizing radiation sources will be stored.

The management of the INPP, realizing the importance of physical security, assumes responsibility for the activities of the enterprise in the field of the INPP physical security and undertakes the following:

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

2. To allocate the necessary resources for the implementation of the set purposes and tasks of physical security.

3. To comply with all legal requirements for physical security applied to the enterprise. Understanding, that only the established procedures and their strict observance can ensure physical security, undertakes to include urgently the provisions of physical security requirements established by the legal acts of the Republic of Lithuania into the normative and technical documents valid at the enterprise and regulating the INPP physical safety.

4. To ensure a flexible and balanced physical security system for the INPP designed for the specific perceived threat defined by VATESI for the enterprise. To review and evaluate the physical security system as the perceived threat changes. If non-conformities or violations are identified, to strive for the elimination of them as soon as possible with the implementation of organizational and technical measures.

5. To ensure implementation of the principles established by the IAEA Nuclear Security Series, No. 20 (Nuclear Security Fundamentals, No. 20 – Objective and Essential Elements of a State's Nuclear Security Regime).

6. To analyze the division of the INPP nuclear facilities into the protected zones, periodically conduct the comprehensive evaluation of the INPP physical security system, including the actions of the licensee, security and reacting forces and, if necessary, other physical security subjects.

7. To formulate the cybernetic security policy at the enterprise and organize its implementation.

8. To monitor the cybernetic space of the information infrastructure of the enterprise, to analyse the state of cybernetic security of the information infrastructure of the enterprise, to evaluate the emerging cybernetic threats, risks and the possibility of violations.

9. To carry out the development of the cybernetic security culture at the enterprise.

10. To strengthen the cybernetic defence of the enterprise by introducing advanced organizational and technical measures for cybernetic security.

11. To ensure that all personnel working at the nuclear facility, as well as at the nuclear facility site, also employees of contractor organizations understand the importance of physical security, safety and security culture, and consciously comply with established requirements.

The enterprise, taking responsibility for the results of its activities, and to ensure physical security, chooses the best means in its activities and attracts highly qualified specialists.

The management of the enterprise is obliged to ensure that the INPP physical security policy will be accessible, known and understandable to every employee of the enterprise.

The evaluation of this policy is carried out annually during the analysis of the productivity and effectiveness of the INPP management system.

The INPP physical security policy is changed or annulated by the order of the INPP Director General.

_____

AGREED by
VATESI letter No. *(15.1E-33) 22.1-240* of *08-04-2020*

Developed by
Head of PSOD
Marius Pernavas, tel.29856

Э.Б., 1, 25-05-2020

Translated by
Ema Banevičienė,
Translator of
Document Management Division of
SE Ignalina NPP,
25-05-2020