HEAD OF THE STATE NUCLEAR POWER SAFETY INSPECTORATE

ORDER
APPROVING THE NUCLEAR SAFETY REQUIREMENTS BSR-1.6.3-2024 "CYBER SECURITY ASSURANCE AT NUCLEAR FACILITIES"

15 January 2024 No.22.3-11
Vilnius

Pursuant to Article 22(1)(3) of the Republic of Lithuania Law on Nuclear Energy and Article 4(1), (2) and (9) of the Republic of Lithuania Law on Nuclear Safety, I hereby:

1. Approve the Nuclear Safety Requirements BSR-1.6.3-2024 "Cyber Security Assurance at Nuclear Facilities" (attached).

2. Establish that this Order shall come into force on 1 May 2024.

Head Michail Demčenko

APPROVED by
Order No. 22.3-11 of the Head of the State Nuclear Power Inspectorate of 15 January 2024

NUCLEAR SAFETY REQUIREMENTS BSR-1.6.3-2024 "CYBER SECURITY ASSURANCE AT NUCLEAR FACILITIES"

CHAPTER I GENERAL PROVISIONS

1. Nuclear Safety Requirements BSR-1.6.3-2024 "Cyber Security Assurance at Nuclear Facilities" (hereinafter referred to as the "Requirements") shall regulate the measures for ensuring cyber security at nuclear facilities and shall be mandatory for an economic entity seeking to obtain or holding licences referred to in Article 22(1)(1) to (5) of the legal act referred to in subparagraph 6.2 of the Requirements (hereinafter referred to as the "Organisation").

2. These Requirements shall apply *mutatis mutandis* to economic entities providing services to the Organisation.

3. The Requirements shall apply to the critical information infrastructure managed by the Organisation to the extent that they do not conflict with the legal act referred to in subparagraph 6.3 of the Requirements and the implementing legal acts.

4. The Organisation shall develop, implement, maintain and continuously improve cyber security measures for all of the Organisation's nuclear power activities and other activities involving nuclear and nuclear fuel cycle materials. These measures shall ensure:

4.1. the confidentiality, integrity and availability of important to safety electronic information;

4.2. the proper functioning of important to safety software;

4.3. the proper functioning of the equipment at this nuclear facility:

4.3.1. industrial process control systems and their components for the normal operation of technological processes involving radioactive materials;

4.3.2. systems and components that perform safety functions during the normal operation of the nuclear facility, in the event of anticipated operational events and accidents as foreseen in the design of the nuclear facility;

4.3.3. systems and components for management of nuclear or radiological accidents;

4.3.4. fire safety systems of structures, systems and components important to safety;

4.3.5. systems to prevent internal hazards and internal events and/or to mitigate consequences of such events;

4.3.6. systems to prevent external hazards and mitigate consequences of such hazards;

4.3.7. electronic communications, including telephone, industrial communication, industrial television and warning systems, used to ensure the normal operation of a nuclear facility, to manage nuclear or radiological accidents and to organise emergency preparedness;

4.3.8. lighting systems used to manage nuclear or radiological accidents and organise emergency preparedness;

4.3.9. structures, systems and components that support the operation of structures, systems and components that perform safety functions;

4.3.10. equipment for emergency preparedness;

4.3.11. radiation control systems to monitor workplaces and workers' exposure;

4.3.12. radiation monitoring systems to ensure radiological monitoring of the environment;

4.3.13. physical security systems;

4.3.14. nuclear material accounting and control systems.

5. It is recommended that the International Atomic Energy Agency (IAEA) publications be taken into account when developing, implementing and improving cyber security measures:

5.1. Implementing Guide "Computer Security for Nuclear Security", IAEA Nuclear Security Series No. 42-G, 2021;

5.2. Technical Guidance "Computer Security Techniques for Nuclear Facilities", IAEA Nuclear Security Series No 17-T, 2021 (Rev. 1);

5.3. Technical Guidance "Computer Security of Instrumentation and Control Systems at Nuclear Facilities", IAEA Nuclear Security Series No 33-T, 2018;

5.4. Document "Computer Security Incident Response Planning at Nuclear Facilities", IAEA-TDL-005, IAEA, 2016;

5.5. Document "Conducting Computer Security Assessments at Nuclear Facilities", IAEA-TDL-006, IAEA, 2016;

5.6. Document "Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain", IAEA-TDL-011, IAEA, 2022.

CHAPTER II
REFERENCES

6. The Requirements contain references to the following legislation:

6.1. Republic of Lithuania Law on Nuclear Energy;

6.2. Republic of Lithuania Law on Nuclear Safety;

6.3. Republic of Lithuania Law on Cyber Security;

6.4. Republic of Lithuania Law on Radiation Protection;

6.5. Republic of Lithuania Law on Electronic Communications;

6.6. Nuclear Safety Requirements BSR-1.4.1-2016 "Management System", approved by Order No. 22.3-56 of the Head of the State Nuclear Power Safety Inspectorate (hereinafter referred to as "VATESI") of 21 June 2010 approving the Nuclear Safety Requirements BSR-1.4.1-2016 "Management System";

6.7. Nuclear Safety Requirements BSR-1.8.11-2021 "Electric power supply to a nuclear facility", approved by Order No. 22.3-118 of the Head of the State Nuclear Power Safety Inspectorate of 23 July 2021 approving the Nuclear Safety Requirements BSR-1.8.11-2021 "Electric power supply to a nuclear facility";

6.8. Nuclear Safety Requirements BSR-1.9.1-2017 "Standards for the release of radionuclides into the environment from nuclear facilities and requirements for the radionuclide release plan", approved by Order No. 22.3-198 of the Head of the State Nuclear Power Safety Inspectorate of 31 October 2017 approving the Nuclear Safety Requirements BSR-1.9.1-2017 "Standards for the release of radionuclides into the environment from nuclear facilities and requirements for the radionuclide release plan";

6.9. Nuclear Safety Requirements BSR-1.6.1-2019 "Physical security of nuclear facilities, nuclear facility sites, nuclear and nuclear fuel cycle materials", approved by Order No. 22.3-37 of the Head of the State Nuclear Power Safety Inspectorate of 4 April 2012 approving the Nuclear Safety Requirements BSR-1.6.1-2019 "Physical security of nuclear facilities, nuclear facility sites, nuclear and nuclear fuel cycle materials".

CHAPTER III
DEFINITIONS

7. 10. For the purposes of the Requirements:

7.1. **Cyber security of nuclear facilities** (hereinafter referred to as "cyber security") shall mean a set of legal, information dissemination, organisational and technical measures aimed at maintaining resilience against factors that threaten the availability and authenticity of electronic information transmitted or processed by or through communication and information systems in

cyberspace, the integrity and confidentiality of information and communication technology-based equipment (e.g. computers, digital controllers, micro-controllers), the smooth operation or control of equipment controlled by a nuclear facility and the restoration of the normal operation of that equipment.

7.2. For the purposes of the Requirements, the terms "management of the Organisation" and "security culture" shall be understood as defined in the legal act referred to in subparagraph 6.6 of the Requirements.

7.3. For the purposes of the Requirements, the terms "emergency preparedness", "nuclear accident", "nuclear facility", "operating organisation" and "design basis threat" shall be understood as defined in the legal act referred to in subparagraph 6.1 of the Requirements.

7.4. For the purposes of the Requirements, the terms "nuclear material" and " structures, systems and components of a nuclear facility important to safety" shall be understood as defined in the legal act referred to in subparagraph 6.2 of the Requirements.

7.5. For the purposes of the Requirements, the terms "critical information infrastructure", "cyber security", "cyber incident", "cyber incident management", "communication and information system" and "industrial process control system" shall have the meaning given to them in the legal act referred to in subparagraph 6.3 of the Requirements.

7.6. For the purposes of the Requirements, the terms "accident foreseen in the design of a nuclear facility", "nuclear and radiological accident management", "external hazard", "principle of defence in depth", "safety function", "system", "component", "support system for structures, systems and components", "internal accident" and "internal hazard" shall be understood in the sense as defined in the legal act referred to in subparagraph 6.7 of the Requirements.

7.7. For the purposes of the Requirements, the term "radioactive material" shall have the meaning given to it in the legal act referred to in subparagraph 6.4 of the Requirements.

7.8. For the purposes of the Requirements, the term "physical security system" shall have the same meaning as in the legal act referred to in subparagraph 6.9 of the Requirements.

7.9. For the purposes of the Requirements, the term "anticipated operational event" shall have the same meaning as in the legal act referred to in subparagraph 6.8 of the Requirements.

7.10. For the purposes of the Requirements, the term "electronic communications" shall have the same meaning as in the legal act referred to in subparagraph 6.5 of the Requirements.

7.11. For the purposes of the Requirements, the term "maintenance" shall have the same meaning as in the legal act referred to in subparagraph 6.7 of the Requirements.

7.12. For the purposes of the Requirements, the term "information resources" shall be understood as the totality of electronic information and the information technology tools that process it, including computerised equipment, managed by the Organisation.

7.13. For the purposes of the Requirements, the term " software important to safety" shall be understood as software installed on work desktop computers, laptops or other devices that is designed for the analysis, calculation, display or other use of data important to safety (e.g. radiation doses, parameters relevant for nuclear safety).

7.14. For the purposes of the Requirements, the term "operational technologies" shall include industrial control systems, among them supervisory control and data acquisition (SCADA) systems, programmable logic controllers (PLCs), distributed control systems (DCS), and other information and communication technology-based technological or ancillary equipment, the primary function of which is not the transmission, storage or processing of information.

7.15. For the purposes of the Requirements, the term "computerised equipment" shall be understood as the equipment referred to in subparagraph 4.3 of the Requirements, which is controlled by equipment based on information and communication technologies (for example, computers, digital controllers or microcontrollers). Computerised equipment may consist of systems of operational technologies, other communication and information systems or be a part of such systems.

7.16. Other terms used in these Requirements shall be understood as defined in the legal acts of the Republic of Lithuania regulating nuclear safety, radiation protection and physical safety of nuclear facilities.

CHAPTER IV
GENERAL REQUIREMENTS FOR CYBER SECURITY ASSURANCE IN AN ORGANISATION

8. The Organisation shall designate a person to be responsible for organising and ensuring cyber security within the Organisation.

9. The Organisation shall ensure that the Organisation's information resources are used only by those persons who have been granted that right in accordance with the procedures established by the Organisation.

10. The Organisation shall ensure that the Organisation's computerised equipment is used, operated and maintained only by persons authorised in accordance with the Organisation's procedures.

11. The Organisation shall promote and develop a culture of cyber security as an integral part of the security culture.

12. The Organisation shall:

12.1. Assess the impact of the Organisation's information resources on the safety of the Organisation's operations, as determined by the Organisation. The Organisation shall review this assessment periodically, but not less than once every three years, and update the same as necessary;

12.2. taking into account the cyber threats identified in the design basis threat document and the characteristics, motivations and intentions of the perpetrators, conduct a vulnerability assessment of the information resources identified as critical to the safety of the nuclear facility in accordance with the assessment referred to in subparagraph 12.1 of these Requirements, and identify the information resources that need to be protected. This assessment shall be updated by the Organisation when the assessment referred to in subparagraph 12.1 of these Requirements is updated;

12.3. implement and maintain preventive organisational and technical measures to ensure the cyber security of information resources identified in accordance with subparagraph 12.2 of these Requirements.

13. The Organisation shall ensure that access to communication and information systems facilities and computerised equipment and controls is restricted to those persons who have been granted such access in accordance with the procedures established by the Organisation. These measures shall be implemented and maintained in a proportionate manner, taking into account the assessments referred to in subparagraphs 12.1 and 12.2 of the Requirements.

14. The Organisation shall ensure that cyber incident management and lessons learned in cyber incident management are applied to the implementation and maintenance of organisational and technical cyber security measures.

15. The Organisation shall regularly review the effectiveness of its cyber security measures at the times and in accordance with the procedures set out in the management system documents. In addition, the Organisation shall organise cyber security exercises and/or participate in cyber security exercises organised by other competent organisations in order to validate the effectiveness of technical and organisational cyber security measures.

16. The Organisation shall ensure that products or services received from information technology suppliers comply with these Requirements, other nuclear safety normative technical documents and the Organisation's management documents that address cyber security aspects.

CHAPTER V
CYBER SECURITY MANAGEMENT

17. The Organisation shall establish cyber security policies and processes as part of the Organisation's management system established in accordance with the legal act referred to in subparagraph 6.6 of the Requirements. Cyber security policies and processes shall ensure that the objectives set out in paragraph 4 of the Requirements are achieved. The cyber security policy shall

be approved by management of the Organisation. Cyber security policies and processes shall be documented, continuously evaluated and improved.

18. The cyber security policy and its implementing documents shall be consistent with the physical security and nuclear safety policies of the Organisation.

19. The documents implementing the cyber security policy shall set out:

19.1. general aspects:

19.1.1. application, approval and use of the cyber security policy and its implementing documents;

19.1.2. allocation of the Organisation's resources for cyber security;

19.1.3. links with other processes in the Organisation;

19.1.4. improvement of the Organisation's cyber security state;

19.1.5. periodic review of the cyber security policy and its implementing documents;

19.2. aspects of personnel management:

19.2.1. establishment of responsibilities and competences related to cyber security;

19.2.2. management of recruitment, redeployment and dismissal of personnel;

19.2.3. setting up of groups of information resource users, and granting and management of rights and access to such resources;

19.2.4. cyber security advice and training for the staff;

19.2.5. promotion and development of the cyber security culture;

19.2.6. links with other human resource management processes in the Organisation;

19.3. assessment of risks, vulnerability and compliance:

19.3.1. assessment and periodic evaluation of threats and vulnerabilities related to information resources;

19.3.2. procedures and documentation of cyber security audits;

19.4. management of cyber security of information resources:

19.4.1. documentation of cyber security measures;

19.4.2. creation, protection and change of usernames and passwords for users of information resources;

19.4.3. use of a wireless network;

19.4.4. use of email;

19.5. secure use and control of mobile devices used to access information resources:

19.5.1. encryption settings for data on mobile devices;

19.5.2. use of information resources outside the Organisation and/or on mobile devices;

19.6. intrusion detection and prevention:

19.6.1. testing of the effectiveness of cyber security measures and cyber security exercises;

19.7. cyber incident management:

19.7.1. organisation of cyber incident management, including the identification, assessment, containment, remediation and restoration of normal operations of the Organisation;

19.7.2. assessment and use of lessons learned in cyber incident management to improve cyber security.

20. The Organisation shall ensure that it has at all times sufficient qualified personnel to ensure the effectiveness of its cyber security measures and compliance with these Requirements, other nuclear safety normative technical documents and the Organisation's management documents governing cyber security aspects.

21. The Organisation shall establish and document cyber security competency requirements for all staff members with access to information resources, based on their individual roles.

22. Cyber security competence shall be maintained and improved through training or other measures. The Organisation shall evaluate the effectiveness of training or other measures to maintain or improve the cyber security competence of its staff members.

23. The Organisation shall ensure that staff performing security functions understand the risks and potential consequences of cyber incidents and are able to deal with them appropriately.

24. The staff responsible for cyber security within the Organisation shall have the education, skills, knowledge and/or experience appropriate to the duties of the position, the minimum requirements of which shall be specified in the staff job descriptions.

CHAPTER VI
CYBER SECURITY ASSURANCE IN THE DESIGN, QUALIFICATION AND OPERATION OF COMPUTERISED EQUIPMENT

25. Computerised equipment shall be designed and operated in such a way that the performance of its ancillary functions (e.g. diagnostics, testing, provision of additional information) does not compromise the provision of cyber security.

26. The effectiveness of the cyber security measures for computerised equipment shall be verified when a nuclear facility is commissioned and when cyber security-related modifications to the nuclear facility are made.

27. Cyber security measures shall not interfere with the operation of safety-critical systems and components.

CHAPTER VII
MEASURES TO ENSURE THE CYBER SECURITY OF OPERATIIONAL TECHNOLOGY

28. In order to protect the operational technology against cyber incidents, the following preventive cyber security measures shall be applied in accordance with the principle of proportionality and taking into account the assessments referred to in subparagraphs 12.1 and 12.2 of the Requirements:

28.1. cyber security zones shall be included in the design of the operational technology and, in line with the principle of defence in depth, multi-level cyber security measures shall be developed in these zones. The choice of cyber security zones and the number of protection levels within them shall take into account the importance of the equipment for safety assurance;

28.2. prohibiting data traffic from external electronic communication networks from entering the cyber security zone. Priority shall be given to the use of hardware in the implementation of this measure;

28.3. physical disconnection of the operational technology from public communication networks;

28.4. restricting remote management and service access to the operational technology, including prohibition if necessary for cyber security assurance, and controlling access;

28.5. controlling user access to operating system functions (e.g. use of usernames and passwords, digital identification of users by personal card);

28.6. approval of modifications to operational technology parameters (e.g. change of setpoints) by two or more staff members, which shall be secured by technical access control measures;

28.7. monitoring and logging actions in the operating software;

28.8. prohibiting or controlling the physical connection of external data storage devices (such as USB sticks) and other external devices to the operating system;

28.9. prohibiting wireless connections (e.g. Wi-Fi, Bluetooth) to the operational technology;

28.10. controlling modifications to software (firmware) of operational technology.

CHAPTER VIII
MEASURES TO ENSURE THE CYBER SECURITY OF COMMUNICATION AND INFORMATION SYSTEMS

29. In order to protect communications and information systems, in accordance with the principle of proportionality and taking into account the assessments referred to in subparagraphs 12.1 and 12.2 of the Requirements, the Organisation shall ensure that:

29.1. all communication and information systems workstations and computerised workstations have virus and malicious code detection and removal software installed and regularly updated to scan computers and external storage media. Information system components without malware detection tools may be operated if the risk assessment confirms that the risk of vulnerability of these components is acceptable;

29.2. the installation, maintenance and troubleshooting of communication and information systems shall be carried out only by suitably qualified technicians in accordance with the manufacturer's recommendations;

29.3. only software that is legal and necessary for the performance of their job functions shall be used in communications and information systems;

29.4. the premises housing the technical equipment for communication and information systems shall be provided with the operating conditions specified by the manufacturer, and the equipment shall be maintained and operated in accordance with the equipment manufacturer's recommendations;

29.5. computerised equipment for information systems shall be equipped with a voltage filter and an uninterruptible power supply to ensure the operation of the computerised equipment and to protect against voltage fluctuations.

30. The Organisation shall apply the following measures to ensure the cyber security of system and application software:

30.1. only legal, authorised and secure system and application software shall be used;

30.2. installation, maintenance and troubleshooting of the software shall be carried out only by suitably qualified professionals;

30.3. software configuration shall be password protected;

30.4. updates recommended by the manufacturers of the operating system and other software (such as anti-virus and anti-malware software) for the computer equipment on users' workstations shall be promptly tested and installed;

30.5. software tools shall be in place to identify users and administrators and their actions.

31. The Organisation shall apply the following measures to ensure the cyber security of the data transmission network:

31.1. service stations, computerised workstations and other computer equipment connected to the electronic information network shall be separated from public telecommunication networks. Firewalls shall be used if the equipment needs to be connected to public telecommunication networks. In this case, firewalls shall be enabled on the information systems' service stations and configured to allow only data traffic related to the functionality and administration of the information systems;

31.2. firewall logs shall be analysed regularly and firewall security rules shall be reviewed and updated periodically;

31.3. connection to computerised equipment information systems from public telecommunication networks shall be strictly controlled and shall be carried out only via proxy servers. Data transfer shall only be possible using secure encrypted communication channels (VPN, SSL);

31.4. filters shall be used to protect the perimeter of the network of information systems for computerised equipment to protect the computer equipment of users of information systems browsing email and the public communication network against malicious code;

31.5. wireless network security and control:

31.5.1. only wireless network devices that meet the technical requirements for cyber security, as agreed with the person responsible for organising and ensuring cyber security within the Organisation or another authorised employee of the Organisation shall be used;

31.5.2. wireless access points shall only be deployed in a separate subnet in a controlled area;

31.5.3. EAP / TLS (Extensible Authentication Protocol or Transport Layer Security) protocol shall be used when connecting to a wireless network;

31.5.4. the use of SNMP (Simple Network Management Protocol) on the wireless interface shall be disabled;

31.5.5. all unnecessary control protocols shall be disabled;

31.5.6. TCP (Transmission Control Protocol) / UDP (User Datagram Protocol) ports not in use shall be disabled;

31.5.7. peer-to-peer functionality, which prevents wireless devices from communicating with each other, shall be banned;

31.5.8. the wireless connection shall be encrypted with a key of at least 128 bits;

31.5.9. the manufacturer's standard keys shall be changed at the wireless access station before encryption of the wireless connection can begin;

31.6. communication cables shall be protected against unauthorised access or damage.

CHAPTER IX
FINAL PROVISIONS

32. Any person who violates the Requirements shall be liable in accordance with the procedure established by the laws of the Republic of Lithuania.

_____