KOZLODUY NPP EAD
CYBERSECURITY MANAGEMENT POLICY

The Cybersecurity Management Policy establishes the framework for achieving a high overall level of cybersecurity at Kozloduy NPP EAD in its capacity as an essential entity and a critical entity of significance to the national security.

THE CYBERSECURITY MANAGEMENT POLICY AIMS AT ACHIEVING THE FOLLOWING OBJECTIVES:

- Ensuring network and information security in order to achieve availability, authenticity, integrity, and confidentiality of information within the Company
- Effectively preventing threats and minimising incidents related to cybersecurity
- Ensuring the continuity of systems critical to the Company's business
- Ensuring cybersecurity throughout the supply chain.

CYBERSECURITY IN THE COMPANY IS BUILT ON THE FOLLOWING PRINCIPLES:

- Compliance with international and national legislation, regulatory and contractual requirements in accordance with the Company's business objectives
- Prevention and timeliness through 'defence in depth' at all levels of the information infrastructure
- Risk-based approach to minimise impact
- Resilience of processes affecting information assets
- Continuous training on cybersecurity and cyber hygiene
- Preparedness for crisis response
- Systematic monitoring, performance analysis, and learning lessons for continuous enhancement.

Kozloduy NPP EAD managers at all levels are committed to providing and enhancing the level of cybersecurity bearing the responsibility for the implementation of the requirements regarding protection of all information and communication assets against internal, external, intentional, and accidental threats, as well as for ensuring the business continuity.

The Cybersecurity Management Policy is communicated to all the Company's employees and each and every one of them is responsible for the implementation of its principles in their efforts towards achieving the set objectives.