TSAKOS ENERGY NAVIGATION LIMITED

CYBERSECURITY POLICY

1. The Scope of the Policy

A. This Cybersecurity Policy (the "Policy") applies to all directors, officers, contractors, and employees of: (1) Tsakos Energy Navigation Limited ("TEN") and its subsidiaries and other business entities controlled by it (collectively, the "Company"); (2) Affiliates and entities that regularly provide management or other services to the Company, including but not limited to Tsakos Energy Management Limited and Tsakos Shipping & Trading S.A. (each a "Management Company" and collectively the "Management Companies"); Collectively, the Company and the Management Companies are referred to as "Covered Persons."

B. Compliance with this Policy is required and is an ongoing responsibility of all Covered Persons.

2. Risk Management and Strategy

A. Integration of Cyber Risk Management

In the rapidly evolving landscape of modern maritime operations, cybersecurity is a vital enabler. Recognizing the need to integrate cyber risk management into our safety management system, the Company commits to:

- Adequate investment in security technologies, systems, processes, and personnel;
- Ongoing review and updates to our cybersecurity strategy, prioritizing key risk areas due to vulnerabilities in our global supply chain ecosystem and the volatile geopolitical environment.

B. Key Components of Cybersecurity Risk Management

1. **Employee Training and Awareness**
   - Conduct regular training sessions and awareness programs to reinforce our Acceptable Use Policies;
   - Emphasize the crucial role of human behavior in defending against cyber threats.
2. **Technical Measures**
   - Implement industry-accepted technical safeguards, including network configurations, access controls, and detection software;
   - Fortify systems against cyber incidents with robust technological defenses.
3. **Continuous Monitoring**
   - Employ ongoing monitoring mechanisms to track internal and external cybersecurity threats;
   - Ensure timely response and mitigation of identified threats.
4. **Knowledge Sharing**
   - Engage in webinars, seminars, and forums to gather and disseminate threat intelligence;
   - Enrich internal audit and compliance efforts with shared knowledge.

5. **Third-party Evaluations**
    - Conduct periodic assessments by external consultants to evaluate the effectiveness of security controls;
    - Identify and address potential vulnerabilities through external feedback.

C. Regular Audits and Incident Response

- Conduct regular internal and external audits and reviews of our cybersecurity policies and controls;
- Promptly report, assess, and escalate incidents as necessary;
- Maintain incident response processes geared towards minimizing impact and ensuring business continuity.

3. Governance

A. Oversight Structure

- Ensure oversight of cybersecurity risks through governance structures, with findings and recommendations reported to the Audit Committee (AC) of the Board of Directors and Management;
- The Audit Committee oversees cybersecurity risks and incidents, ensuring compliance with disclosure requirements, collaborating with law enforcement, and addressing related financial and operational risks;
- Management regularly discusses cyber risks and trends with the audit committee.

B. SEC Disclosure

- Required and appropriate disclosure related to cybersecurity, including material cybersecurity incidents and risks related to any failure to protect our information systems against security breaches shall be made in TEN's reports filed with the U.S. Securities and Exchange Commission, including Item 16K of the Form 20F.

This Policy is subject to regular review and updates to ensure alignment with emerging cybersecurity threats and best practices. All Covered Persons are expected to adhere to the guidelines and procedures outlined herein to safeguard the Company's information systems and assets.