Announcement of Global Power Synergy Public Company Limited

No. 007 / 21

Cybersecurity Policy

In order to ensure the effectiveness of Global Power Synergy Public Company Limited (GPSC)'s cybersecurity and cyber risk management, as well as compliance with relevant international standards that aim to protect GPSC from cyber threats, attacks, destroying, and thefts, Section 3 "Cyber Security Policy" in the Information and Communication Technology Policy Standard Practice B.E. 2563 has now been annulled and substituted with this Cybersecurity Policy which is established as follows:

1. Establish cybersecurity working committee comprising function representatives who are responsible for cybersecurity business process and operation process in each area. The working committee will be assigned roles, responsibilities and management approaches.

2. Develop and maintain cybersecurity framework and practices to comply with relevant international standards. Regularly monitor related laws and regulations regarding cybersecurity and ensure compliance at least once a year.

3. Implement cybersecurity risk management by identifying threats and vulnerabilities, and assessment of likelihoods and impacts to GPSC business. Also establish cybersecurity risk responses on such threats and vulnerabilities regarding Enterprise Risk Management which covers all assets and human resources of both GPSC and related external parties.

4. Conduct internal communication and trainings regarding cybersecurity to promote and increase GPSC employees' awareness, responsibility and understanding about cybersecurity and to handle cyber threats regularly or at least once a year.

5. Implement protection and detection systems to respond to cyber-attacks covering all GPSC information systems. Establish monitoring systems and assign responsible parties related to cybersecurity to monitor and report cyber threats to GPSC executive management at least once a quarter.

/6. Establish…

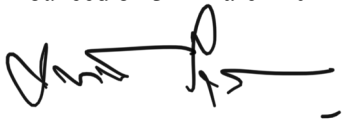
6. Establish cybersecurity incident response plans to handle any abnormal activities or incidents promptly and efficiently, as well as to reduce the adverse impacts to GPSC's key business processes. The plans shall be tested and reviewed regularly or at least twice a year.

7. Establish cybersecurity incident recovery plans, designed to reduce adverse impacts to GPSC's key business processes. The plans shall also be tested, reviewed and evaluated for accuracy and efficiency regularly or at least once a year.

8. Vulnerability assessment or penetration test shall be conducted covering infrastructure and applications of all GPSC information systems that are exposed to cyber risks regularly or at least once a year.

This shall be effective from 1st April 2021.

Announced on 31st March 2021



(Mr. Worawat Pitayasiri)

President and Chief Executive Officer