



IRPC Public Company Limited

Cyber Security Policy

2026

To ensure that the information systems, data protection, digital assets, digital technologies, and critical digital infrastructure of IRPC Public Company Limited are adequately protected against cyber threats and that cyber risks are effectively managed, the Company is committed to strengthening stakeholder confidence, supporting business continuity, and enhancing its sustainable competitiveness in alignment with internationally recognized cybersecurity frameworks, standards, and best practices. The Company therefore establishes the Cyber Security Policy as follows:

1. Establish a clear cybersecurity governance structure, including defined roles, responsibilities, and accountabilities, while allocating appropriate resources, setting performance indicators, and monitoring cybersecurity performance in alignment with the Company's business objectives and risk appetite.

2. Comply with applicable cybersecurity laws, regulations, standards, and requirements, while monitoring regulatory changes and continuously improving cybersecurity controls and governance through assessment results, audit findings, and lessons learned from cybersecurity incidents.

3. Establish systematic processes to identify, assess, monitor, and manage cyber risks using a risk-based approach in order to prevent cyber threats, minimize potential impacts, and strengthen the Company's cyber resilience.

4. Establish capabilities to continuously monitor, detect, analyze, report, and respond to cybersecurity incidents in a timely manner, together with appropriate containment, remediation, recovery, and post-incident review processes to continually enhance cybersecurity response effectiveness.

5. Establish and maintain Business Continuity Plans (BCP), Information Technology Disaster Recovery Plans (ITDRP), and Cyber Crisis Management capabilities, including regular testing, exercises, reviews, and continuous improvement to ensure the Company's ability to effectively respond to disruptive cyber events.

6. Establish appropriate measures to protect information, information systems, and digital assets through information classification, access control based on the Need-to-Know and Least Privilege principles, secure authentication mechanisms, and appropriate security controls to preserve the confidentiality, integrity, and availability of information.

7. Integrate cybersecurity requirements throughout the lifecycle of the development, acquisition, enhancement, and operation of information systems, digital technologies, Operational Technology (OT), cloud environments, Internet of Things (IoT) devices, and emerging technologies in accordance with the principles of Security by Design and Secure by Default.

8. Monitor, analyze, and leverage Cyber Threat Intelligence to strengthen the Company's capabilities to prevent, detect, and respond to evolving cyber threats proactively and effectively.

9. Establish processes to assess, monitor, and oversee the cybersecurity practices of service providers, business partners, contractors, suppliers, and other relevant third parties to ensure that appropriate security controls and cyber risk management measures are implemented throughout the Company's supply chain in accordance with the Company's requirements.

10. Promote a strong cybersecurity culture by continuously enhancing the knowledge, awareness, and capabilities of directors, executives, employees, and relevant stakeholders through communication, training, and capability development, enabling everyone to actively participate in cybersecurity risk management with responsibility and accountability.

11. Regularly monitor, review, assess, and evaluate the effectiveness of the Cyber Security Management System to continuously strengthen the Company's ability to prevent and respond to evolving cyber threats and to support sustainable organizational development.

This Policy shall apply to all business units of IRPC Public Company Limited and its subsidiaries, as well as directors, executives, employees, suppliers, business partners, contractors, service providers, and other relevant parties who access the Company's information, information systems, or digital assets. All such parties are required to comply with this Policy, uphold its principles, demonstrate responsible conduct, and support the Company's commitment to good corporate governance, enterprise risk management, and sustainable organizational development.

Announced and effective on 15 September 2026



(Asst. Prof. Dr. Chaiyaporn Puprasert)

Chairman

Note: This Policy has been approval by the Board of Directors, at the meeting number 10/2026 on 21 July 2026