

Announcement of PTT Public Company Limited
Subject: Information Security Management System Policy

.....

To ensure that the information systems of PTT Public Company Limited are appropriately and efficiently managed in accordance with international standards, and to comprehensively address the key components of information security consisting of Confidentiality, Integrity, and Availability or CIA as well as to prevent potential issues arising from improper use of information technology and various threats, PTT hereby establishes its Information Security Management System Policy with the following key principles:

1. To build confidence and ensure the security and effectiveness of information system usage.
2. To define the scope of information security management system based on ISO/IEC 27001 standards and to continuously review and improve this scope.
3. To establish requirements and guidelines for maintaining information security.
4. To ensure that executives, employees, system administrators, and external personnel working with PTT recognize the importance of information security in their operations.
5. To conduct risk assessments and manage information security risks to prevent threats that may impact PTT's business operations.
6. To analyze incidents that cause damage or loss to information systems, including information leakage, in order to develop preventive and corrective measures.

This policy applies to all departments within PTT. All executives, employees, and personnel working with PTT must understand and comply with this policy. Executives at all levels must lead by example and actively support and promote its effective implementation.

Announced on 4 October 2562



ประกาศ บริษัท ปตท. จำกัด (มหาชน)

เรื่อง นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

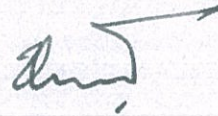
(Information Security Management System Policy)

เพื่อให้ระบบสารสนเทศของบริษัท ปตท. จำกัด (มหาชน) (“ปตท.”) เป็นไปอย่างเหมาะสม มีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล และครอบคลุมองค์ประกอบด้านความมั่นคงปลอดภัยสารสนเทศ ที่ประกอบไปด้วย การรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความพร้อมใช้งาน (Availability) หรือหลัก CIA รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและภัยคุกคามต่าง ๆ จึงสมควรกำหนดให้มีการบริหารจัดการความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของ ปตท. โดยมีสาระสำคัญดังต่อไปนี้

1. สร้างความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศให้มีประสิทธิภาพและประสิทธิผล
2. กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ โดยอ้างอิงมาตรฐาน ISO/IEC 27001 และพิจารณาปรับปรุงขอบเขตดังกล่าวอย่างต่อเนื่อง
3. จัดให้มีข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศเพื่อวางหลักเกณฑ์แนวทางเกี่ยวกับการรักษาความปลอดภัยของสารสนเทศ
4. ผู้บริหาร พนักงาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับ ปตท. ต้องตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศของ ปตท. ในการดำเนินงาน
5. จัดให้มีการประเมินความเสี่ยงและบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันภัยคุกคามต่าง ๆ ที่อาจจะส่งผลกระทบต่อการดำเนินธุรกิจของ ปตท.
6. จัดให้มีการวิเคราะห์เหตุการณ์ต่าง ๆ ที่ก่อให้เกิดความเสียหายหรือสูญเสียของระบบสารสนเทศ รวมทั้งการรั่วไหลของสารสนเทศ เพื่อพิจารณาหาแนวทางแก้ไขและป้องกัน

นโยบายฉบับนี้ ประยุกต์ใช้กับทุกหน่วยงานของ ปตท. ผู้บริหาร พนักงาน และผู้ปฏิบัติงาน
ให้ ปตท. ทุกคนต้องเข้าใจและปฏิบัติตามนโยบาย ฉบับนี้ โดยผู้บริหารในทุกระดับต้องเป็นแบบอย่างที่ดี
รวมทั้งสนับสนุน ผลักดัน ให้เกิดการปฏิบัติอย่างจริงจัง

ประกาศ ณ วันที่ 4 ตุลาคม 2562



(นายชาญศิลป์ ตรีนุชกร)

ประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่