Announcement of PTT Public Company Limited

Subject: Cybersecurity Policy Announcement

……..

To ensure that PTT's information systems are effectively protected against cyber threats and that cybersecurity risks are managed in alignment with international standards and best practices, PTT Public Company Limited hereby establishes the following Cybersecurity Policy with the key principles outlined below:

1. Cybersecurity Responsibility: Departments responsible for cybersecurity must regularly report cyber threat information to the management.
2. Framework Alignment: Develop and maintain cybersecurity frameworks and practices that are consistent with international standards.
3. Risk Management Measures: Implement control measures and manage cybersecurity risks across all information systems that are vulnerable to cyber threats.
4. Intrusion Prevention and Detection: Install comprehensive intrusion prevention and detection systems covering all PTT information systems, with continuous monitoring and regular reporting of audit results.
5. Security Testing: Conduct security testing of information systems prior to deployment, covering both IT infrastructure and application systems.
6. Vulnerability Assessment: Perform vulnerability assessments or penetration testing at least once a year for information systems at risk of cyber threats, including IT infrastructure and application systems.
7. Cybersecurity Awareness Training: Provide regular training and education on potential cyber threats to enhance employee awareness and understanding of cybersecurity response measures.
8. Organizational Responsibility: All departments must foster a sense of responsibility and awareness among employees regarding cybersecurity.

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 implementation.

Announced on 4 October 2562

ประกาศ บริษัท ปตท. จำกัด (มหาชน)

นโยบายการรักษาความมั่นคงปลอดภัยด้านไซเบอร์

(Cyber Security Policy)

เพื่อให้ระบบสารสนเทศของ บริษัท ปตท. จำกัด (มหาชน) (“ปตท.”) มีการป้องกันภัยคุกคามและมีบริหารจัดการความเสี่ยงด้านไซเบอร์อย่างมีประสิทธิภาพ สอดคล้องกับกรอบการดำเนินงานหรือแนวปฏิบัติที่เป็นมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ จึงสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ โดยมีสาระสำคัญ ดังนี้

1. หน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์ ต้องรายงานข้อมูลภัยคุกคามทางด้านไซเบอร์ให้แก่ผู้บริหารรับทราบอย่างสม่ำเสมอ
2. พัฒนาและรักษากรอบการดำเนินงานหรือแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ให้สอดคล้องกับมาตรฐานสากล
3. กำหนดมาตรการควบคุมและบริหารจัดการความเสี่ยงความมั่นคงปลอดภัยด้านไซเบอร์ครอบคลุมระบบสารสนเทศที่มีความเสี่ยงจากภัยคุกคามด้านไซเบอร์
4. ต้องมีการติดตั้งระบบป้องกันและระบบตรวจจับการบุกรุก โดยต้องครอบคลุมระบบสารสนเทศของ ปตท. ทั้งหมด พร้อมทั้งมีการเฝ้าระวัง รายงานผลตรวจสอบอย่างสม่ำเสมอ
5. ต้องดำเนินการทดสอบความมั่นคงปลอดภัยระบบสารสนเทศก่อนให้บริการจริงโดยครอบคลุมระบบโครงสร้างพื้นฐานสารสนเทศ (Infrastructure) และโปรแกรมประยุกต์ (Application)
6. ต้องจัดให้มีการตรวจประเมินช่องโหว่ (Vulnerability Assessment) หรือ การทดสอบเจาะระบบ (Penetration Test) โดยครอบคลุมระบบโครงสร้างพื้นฐานสารสนเทศ (Infrastructure) และโปรแกรมประยุกต์ (Application) สำหรับระบบสารสนเทศที่มีความเสี่ยงจากภัยคุกคามด้านไซเบอร์อย่างน้อยปีละ 1 ครั้ง
7. สื่อความและจัดอบรมให้ความรู้ภัยคุกคามด้านไซเบอร์ (Cybersecurity Awareness) ที่อาจเกิดขึ้นเพื่อสร้างความตระหนักและความรู้ความเข้าใจการรับมือภัยคุกคามทางไซเบอร์ให้กับพนักงานอย่างสม่ำเสมอ
8. ทุกหน่วยงานต้องสร้างความสำนึกในการรับผิดชอบและความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ให้แก่พนักงานอย่างสม่ำเสมอ

/นโยบายฯ ฉบับนี้ .....

นโยบายฯ ฉบับนี้ ประยุกต์ใช้กับทุกหน่วยงานของ ปตท. ผู้บริหาร พนักงาน และผู้ปฏิบัติงาน ให้ปตท. ทุกคน ต้องเข้าใจและปฏิบัติตามนโยบายฯ ฉบับนี้ โดยผู้บริหารในทุกระดับต้องเป็นแบบอย่างที่ดี รวมทั้งสนับสนุน ผลักดัน ให้เกิดการปฏิบัติอย่างจริงจัง

ประกาศ ณ วันที่ 4 ตุลาคม 2562

(นายชาญศิลป์ ตรีนุชกร)

ประธานเจ้าหน้าที่บริหารและกรรมการผู้จัดการใหญ่