บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)
Airports of Thailand Public Company Limited

AOT Announcement

Subject: AOT Cyber Security Policy

(Revised Edition, B.E. 2568 / 2025)

Airports of Thailand Public Company Limited (AOT) is an organization operating airport businesses to provide air transport services in accordance with airport operation standards prescribed by government laws, which align with the standards of the International Civil Aviation Organization (ICAO). AOT has integrated information and communication technology into its services to support corporate management, airport operations, as well as the connection and exchange of information with both public and private sectors. This is done to continuously and efficiently satisfy the services provided to both internal and external stakeholders of AOT.

Therefore, it is essential to prevent and respond to incidents resulting from any unauthorized actions or operations conducted through computers or computer systems. Such incidents may cause damage or impact cyber security, or affect the cyber security of computers, computer data, computer systems, or other computer-system-related data, which consequently affect or potentially pose risks to the operations or services of AOT.

Furthermore, the National Cyber Security Committee has designated AOT as a Critical Information Infrastructure (CII) organization. AOT holds duties and responsibilities as prescribed by law, which include preventing, responding to, and mitigating risks from cyber threats that affect or occur against its critical information infrastructure.

To ensure that AOT maintains cyber security to prevent, respond to, and mitigate risks from both domestic and international cyber threats—which may affect AOT's operations or services, and subsequently impact state security and economic stability—it is deemed appropriate to establish the AOT Cyber Security Policy as follows:

1. Repeal the AOT Announcement regarding the AOT Cyber Security Policy dated April 5, B.E. 2564 (2021).

2. Formulate policies, codes of practice, and standard frameworks for cyber security, including any other documentation required to comply with the Cyber Security Act, B.E. 2562 (2019). Additionally, review the AOT Cyber Security Policy and the AOT Cyber Security Guideline and Standard Framework at least once a year, or when significant changes occur.

3. In the event that a cyber threat occurs, or is anticipated to occur, against the information systems under AOT's supervision, the AOT department responsible for or overseeing such information and communication technology systems shall examine the relevant data, computer data, and AOT's computer systems, as well as surrounding circumstances, to assess whether a cyber threat has occurred. If the examination reveals that a cyber threat has occurred or is anticipated to occur, the department shall take actions to prevent, respond to, and mitigate risks from such cyber threats in accordance with the AOT Cyber Security Guideline and Standard Framework, and promptly notify the Office of the National Cyber Security Committee and AOT's regulatory or supervisory authorities.

4. All levels of AOT employees shall acknowledge and strictly comply with the AOT Cyber Security Policy, as well as the AOT Cyber Security Guideline and Standard Framework. Any violation or breach shall be considered a disciplinary offense according to AOT regulations. In the case of legal violations, it shall be deemed an individual liability.

Announced on April 11, 2025 (B.E. 2568)

(Mr. Kirati Kijmanawat)

President / Chief Executive Officer

บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)
Airports of Thailand Public Company Limited

ประกาศบริษัท ท่าอากาศยานไทย จำกัด (มหาชน)
เรื่อง นโยบายความมั่นคงปลอดภัยไซเบอร์ของ ทอท. (AOT Cyber Security Policy)
ฉบับทบทวนประจำปี 2568

บริษัท ท่าอากาศยานไทย จำกัด (มหาชน) (ทอท.) เป็นองค์กรที่ดำเนินธุรกิจท่าอากาศยาน ในการให้บริการด้านการขนส่งทางอากาศตามมาตรฐานการดำเนินงานสนามบินเป็นไปตามกฎหมายที่รัฐกำหนด ซึ่งสอดคล้องกับมาตรฐานขององค์การการบินพลเรือนระหว่างประเทศ (International Civil Aviation Organization : ICAO) โดย ทอท.ได้นำเทคโนโลยีสารสนเทศและการสื่อสารมาให้บริการเพื่อสนับสนุนด้านการบริหารองค์กร ด้านปฏิบัติการท่าอากาศยาน รวมถึงการเชื่อมโยงแลกเปลี่ยนข้อมูลสารสนเทศกับหน่วยงานทั้งภาครัฐและเอกชน เพื่อตอบสนองการให้บริการผู้มีส่วนได้ส่วนเสีย (Stakeholders) ทั้งภายในและภายนอก ทอท.ได้อย่างต่อเนื่องและมีประสิทธิภาพ จึงจำเป็นต้องมีการป้องกันและรับมือกับเหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใดๆ ที่มิชอบ ซึ่งกระทำผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการดำเนินงานหรือการให้บริการของ ทอท. ประกอบกับคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้ประกาศกำหนดให้ ทอท.เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) โดยมีหน้าที่ความรับผิดชอบตามที่กฎหมายกำหนดไว้ ซึ่งรวมถึงการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

เพื่อให้ ทอท.มีการรักษาความมั่นคงปลอดภัยไซเบอร์ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ ที่อาจก่อให้เกิดผลกระทบต่อการดำเนินงานหรือการให้บริการของ ทอท. ซึ่งส่งผลกระทบต่อความมั่นคงของรัฐ และความมั่นคงทางเศรษฐกิจ จึงเห็นสมควรกำหนดนโยบายความมั่นคงปลอดภัยไซเบอร์ของ ทอท.โดยให้ดำเนินการ ดังนี้

1. ยกเลิกประกาศ ทอท.เรื่อง นโยบายความมั่นคงปลอดภัยไซเบอร์ของ ทอท. (AOT Cyber Security Policy) ลงวันที่ 5 เมษายน พ.ศ. 2564

2. จัดทำนโยบาย ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงเอกสารอื่นใดที่ต้องดำเนินการให้สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และทบทวนนโยบายความมั่นคงปลอดภัยไซเบอร์ของ ทอท. (AOT Cyber Security Policy) และประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอท. (AOT Cyber Security Guideline and Standard Framework) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

3. กรณี...

3. กรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของ ทอท. ให้ส่วนงาน ทอท.ที่มีระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในความรับผิดชอบ หรือกำกับดูแล ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ของ ทอท.รวมถึงพฤติการณ์แวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบพบว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอท.และแจ้งไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และหน่วยงานควบคุมหรือกำกับดูแล ทอท.โดยเร็ว

4. ให้พนักงาน ทอท.ทุกระดับรับทราบและถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยไซเบอร์ของ ทอท. รวมทั้งประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอท. โดยเคร่งครัด ทั้งนี้ การละเมิดหรือฝ่าฝืนถือเป็นความผิดทางวินัยตามระเบียบของ ทอท.และกรณีการกระทำผิดตามกฎหมาย ถือเป็นความผิดเฉพาะส่วนบุคคล

ประกาศ ณ วันที่ 11 เมษายน พ.ศ. 2568

(นายกีรติ กิจมานะวัฒน์)
กรรมการผู้อำนวยการใหญ่