



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

ประกาศบริษัท ท่าอากาศยานไทย จำกัด (มหาชน)

เรื่อง นโยบายความมั่นคงปลอดภัยไซเบอร์ของ ทอท. (AOT Cyber Security Policy)

บริษัท ท่าอากาศยานไทย จำกัด (มหาชน) (ทอท.) เป็นองค์กรที่ดำเนินธุรกิจท่าอากาศยาน ในการให้บริการด้านการขนส่งทางอากาศตามมาตรฐานการดำเนินงานสนามบินเป็นไปตามกฎหมายที่รัฐกำหนด ซึ่งสอดคล้องกับมาตรฐานขององค์การการบินพลเรือนระหว่างประเทศ (International Civil Aviation Organization : ICAO) โดย ทอท. ได้นำเทคโนโลยีสารสนเทศและการสื่อสารมาให้บริการเพื่อสนับสนุนด้านการบริหารองค์กร ด้านปฏิบัติการท่าอากาศยาน รวมถึงการเชื่อมโยงแลกเปลี่ยนข้อมูลสารสนเทศกับหน่วยงานทั้งภาครัฐและเอกชน เพื่อตอบสนองการให้บริการผู้มีส่วนได้ส่วนเสีย (Stakeholders) ทั้งภายใน และภายนอก ทอท. ได้อย่างต่อเนื่องและมีประสิทธิภาพ จึงจำเป็นต้องมีการป้องกันและรับมือกับเหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใดๆ ที่มีขอบ ซึ่งกระทำผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการดำเนินงานหรือการให้บริการของ ทอท.

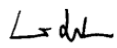
เพื่อให้ ทอท. มีการรักษาความมั่นคงปลอดภัยไซเบอร์ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ ที่อาจก่อให้เกิดผลกระทบต่อการดำเนินงานหรือการให้บริการของ ทอท. ซึ่งส่งผลกระทบต่อความมั่นคงของรัฐ และความมั่นคงทางเศรษฐกิจ จึงเห็นสมควรกำหนดนโยบายความมั่นคงปลอดภัยไซเบอร์ของ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

Airports of Thailand Public Company Limited (AOT) is an organization operating in the airport business, committed to adhering to international aviation operational standards in line with international law and relevant domestic laws. AOT also complies with the standards of the International Civil Aviation Organization (ICAO) by applying information and communication technology to support and enhance the efficiency of aviation operations. This includes managing information systems for stakeholders in aviation to ensure the provision of effective and efficient services.

Given the increasing risks and threats to information systems from cyber threats and security breaches that may affect aviation safety, security, and the trustworthiness of AOT, as well as having potential impacts on national security and the economy, AOT has deemed it necessary to establish the AOT Cyber Security Policy with the following directives:

1. ดำเนินการตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด
2. จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอท.ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว หรือนำประมวลแนวทางปฏิบัติและกรอบมาตรฐานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติไปใช้บังคับ
3. กรณีที่คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติประกาศกำหนดให้ ทอท.เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้ ทอท.มีหน้าที่ความรับผิดชอบตามที่กฎหมายกำหนดไว้ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
4. กรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความรับผิดชอบของ ทอท.ต้องดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ของ ทอท.รวมถึงพฤติกรรมแวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบพบว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอท.และแจ้งไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และหน่วยงานควบคุมหรือกำกับดูแล ทอท.โดยเร็ว
5. ทบทวนนโยบายความมั่นคงปลอดภัยไซเบอร์ของ ทอท.(AOT Cyber Security Policy) และประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอท.อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
6. ให้พนักงาน ทอท.ทุกระดับรับทราบและถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยไซเบอร์ของ ทอท.รวมทั้งประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเคร่งครัด ทั้งนี้ การละเมิดหรือฝ่าฝืนถือเป็นความผิดทางวินัยตามระเบียบของ ทอท.และกรณีการกระทำผิดตามกฎหมายถือเป็นความผิด เฉพาะส่วนบุคคล

ประกาศ ณ วันที่ 5 เมษายน พ.ศ.2564


(นายนิติชัย ศิริสมรรถการ)
กรรมการผู้อำนวยการใหญ่

Announced on: 5 April 2021
Nitinai Sirismatthakarn
President
(Executive Director)

1. Adherence to Laws and Regulations

- Implement cyber security policies and action plans in accordance with national cyber security laws and the requirements of the National Cyber Security Committee.

2. Policy Development

- Formulate policies, action plans, and operational standards for the maintenance of cyber security that are consistent with the policies and plans of the National Cyber Security Committee, or as instructed by relevant government authorities.

3. Risk Management

- In the event of a cyber threat or incident, AOT shall take immediate action to mitigate the risk and report it to the National Cyber Security Committee or relevant authorities, as required.

4. Incident Response

- In cases where a cyber security incident or breach occurs, AOT must investigate, collect relevant data, and implement measures to control, mitigate, and restore the affected systems in compliance with relevant laws and regulations.

5. Review and Update

- Review the AOT Cyber Security Policy, operational standards, and guidelines at least once a year, or whenever significant changes occur.

6. Employee Compliance

- All AOT executives and employees must acknowledge and strictly adhere to the Cyber Security Policy, related operational standards, and guidelines. Any violations will be subject to disciplinary actions and/or legal proceedings, as applicable.