

Document Summary

AOT Cyber Security Policy

The document is an official AOT cybersecurity policy, issued on 5th April 2021. This policy aims to ensure AOT cybersecurity and to reduce potential cybercrime. The policy states six measures with the essence as following:

1. AOT shall comply with cyber security policy and plan according to National Cyber Security Committee **(PDF page 2)**
2. AOT shall prepare with Cyber Security Policy, guidelines and standard of practices accordingly **(PDF page 2)**
3. AOT is responsible for cyber-related risks prevention and reduction should it be appointed by the National Cyber Security Committee **(PDF page 2)**
4. In case of cybercrime, AOT is responsible for reducing cyber risk and reporting to National Cyber Security Committee or other related-authorities **(PDF page 2)**
5. AOT shall regularly review Cyber Security Policy, guidelines and standard of practices at least annually, or when a significant change occurs. **(PDF page 3)**
6. All employees shall acknowledge and strictly adhere to AOT Cyber Security Policy. Disciplinary action shall be taken for violators. Legal violation is the responsibility of individuals. **(PDF page 3)**



บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)
Reports 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 ที่ส่งผลกระทบต่อหรืออาจก่อให้เกิดความเสี่ยงต่อการดำเนินงานหรือการให้บริการของ ทอท.

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

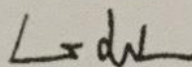
1. ดำเนินการตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด
2. จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอท. ให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว หรือนำประมวลแนวทางปฏิบัติและกรอบมาตรฐานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติไปใช้บังคับ
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. พบพบ...

5. ทบทวนนโยบายความมั่นคงปลอดภัยไซเบอร์ของ ทอท.(AOT Cyber Security Policy) และประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอท.อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

6. ให้พนักงาน ทอท.ทุกระดับรับทราบและถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยไซเบอร์ของ ทอท. รวมทั้งประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเคร่งครัด ทั้งนี้ การละเมิดหรือฝ่าฝืนถือเป็นความผิดทางวินัยตามระเบียบของ ทอท.และกรณีการกระทำผิดตามกฎหมายถือเป็นความผิดเฉพาะส่วนบุคคล

ประกาศ ณ วันที่ 5 เมษายน พ.ศ.2564



(นายนิติชัย ศิริสมรรถการ)

กรรมการผู้อำนวยการใหญ่

AOT
12:11:57:30510131

AOT
12:11:57:30510131