

๑๖ พฤษภาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการ  
ป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

สิ่งที่ส่งมาด้วย รายงานการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ  
ครั้งที่ ๓/๒๕๖๗

ด้วยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ขอเสนอ เรื่อง  
กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกัน  
ข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล มาเพื่อคณะรัฐมนตรีพิจารณาเห็นชอบ โดยเรื่องนี้เข้าข่ายที่จะให้นำเสนอ  
คณะรัฐมนตรีได้ตามพระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘  
มาตรา ๔ (๑)

ทั้งนี้ เรื่องดังกล่าวมีรายละเอียด ดังนี้

#### ๑. เหตุผลความจำเป็นที่ต้องเสนอคณะรัฐมนตรี

การเสนอกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับ  
หน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล มีความจำเป็นต้องเสนอคณะรัฐมนตรี  
เพื่อพิจารณาและให้ความเห็นชอบ เนื่องจากเป็นการดำเนินการตาม พระราชบัญญัติการรักษาความมั่นคง  
ปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๐) ซึ่งกำหนดให้ คณะกรรมการการรักษาความมั่นคง  
ปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่เสนอแนะและให้ความเห็นต่อ คณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคง  
ปลอดภัยไซเบอร์

นอกจากนี้ มาตรา ๒๒ (๕) และ (๖) ของพระราชบัญญัติฉบับเดียวกัน ได้กำหนดให้  
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่ดำเนินการและประสานงาน  
กับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงเฝ้าระวัง ติดตาม  
วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ ซึ่งเป็นหน้าที่สำคัญที่เกี่ยวข้องโดยตรงกับการดำเนินการตาม  
กรอบแนวทางที่เสนอ

ดังนั้น เรื่องนี้จึงเข้าข่ายเรื่องที่ต้องเสนอคณะรัฐมนตรีตาม พระราชกฤษฎีกาว่าด้วยการ  
เสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๔ (๑) เรื่องที่กฎหมายกำหนดให้เป็นอำนาจ  
หน้าที่ของคณะรัฐมนตรีหรือให้ต้องเสนอคณะรัฐมนตรี

#### ๒. ความเร่งด่วนของเรื่อง

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีความจำเป็น  
ที่จะต้องเสนอขอความเห็นชอบและอนุมัติในต่อกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัย  
ไซเบอร์ให้กับหน่วยงานของรัฐจากคณะรัฐมนตรี เนื่องจากปัจจุบันมีการรั่วไหลของข้อมูลส่วนบุคคล  
เป็นจำนวนมาก จึงขอความกรุณาเสนอเรื่องนี้ต่อคณะรัฐมนตรีภายในเดือนมิถุนายน ๒๕๖๘

/๓.สาร...

### ๓. สาระสำคัญและข้อเท็จจริง

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้มีการจัดประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ครั้งที่ ๓/๒๕๖๗ เมื่อวันที่ ๓๐ ตุลาคม ๒๕๖๗ โดยมีวาระที่ ๔.๓ เรื่อง แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้ดำเนินการติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ จึงได้เสนอแนวทางขับเคลื่อนการแก้ไขปัญหาเชิงระบบสำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อเป็นกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ดังนี้

๑) การกำหนดขอบเขตของงานพัฒนาระบบหน่วยงานควรมีการใช้แนวทางมาตรฐาน ISO/IEC 27001 หรือ NIST Cyber Security Framework ในการออกแบบ พัฒนา และบำรุงรักษาระบบงดใช้ข้อมูลจริงในขั้นตอนการพัฒนาระบบ หรือกำหนดให้ใช้ข้อมูลเพื่อทดสอบให้แล้วเสร็จและลบออกภายในระยะเวลา ๓ วัน รวมทั้งกำหนดเกณฑ์สำหรับการเลือกบริษัทพัฒนาซอฟต์แวร์ที่มีประสบการณ์และมาตรฐานที่ผ่านการรับรองทางความปลอดภัย ตลอดจนกำหนดให้มีการกำกับดูแลและติดตาม รวมทั้งการทดสอบความปลอดภัยระบบเป็นประจำ ทั้งในช่วงการพัฒนาและก่อนการใช้งานจริงเพื่อค้นหาช่องโหว่และแก้ไขทันที

๒) หน่วยงานควรจัดการอบรมสำหรับผู้พัฒนาและบุคลากรที่เกี่ยวข้องในเรื่องการออกแบบและพัฒนาระบบให้ปลอดภัย พร้อมสร้างความรับรู้ในเรื่องภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น

๓) จัดให้มีการตรวจสอบและประเมินผลการทำงานของระบบอย่างสม่ำเสมอ รวมถึงการตรวจสอบความสอดคล้องกับมาตรฐานความปลอดภัยที่กำหนด

๔) กำหนดให้มีการระบุเงื่อนไขด้านความปลอดภัยในสัญญาว่าจ้างผู้พัฒนา โดยเน้นความรับผิดชอบต่อปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นจากการพัฒนา

๕) จัดให้มีกลไกการเฝ้าระวังเพื่อแจ้งเตือนและตอบสนองต่อการโจมตีหรือช่องโหว่ที่เกิดขึ้นอย่างรวดเร็ว รวมถึงการมีแผนรับมือเมื่อเกิดเหตุการณ์ความปลอดภัยไซเบอร์

๖) สนับสนุนการปรับปรุงระบบให้ทันสมัยอยู่เสมอ โดยอัปเดตซอฟต์แวร์และแพตช์ด้านความปลอดภัยเมื่อมีช่องโหว่ถูกค้นพบ

๗) หากมีระบบงานที่ไม่ได้ใช้งาน ควรมีการปิดระบบเพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลได้

๘) ให้นำหน่วยงานปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗ ซึ่งสอดคล้องกับนโยบาย Cloud First Policy เพื่อเสริมสร้างความมั่นคงปลอดภัยทางดิจิทัล

ทั้งนี้ ที่ประชุมมีมติ เห็นชอบ แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่ สกมช. เสนอ และมอบหมายให้ สกมช. เสนอแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ให้คณะรัฐมนตรีพิจารณาประกาศให้ทุกหน่วยงานถือปฏิบัติ ต่อไป

#### ๔. ประโยชน์และผลกระทบ

การดำเนินการตามกรอบแนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ จะช่วยยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในภาครัฐอย่างเป็นระบบ ส่งผลให้ระบบดิจิทัลของรัฐบาลมีความมั่นคงปลอดภัยมากยิ่งขึ้น เพิ่มความเชื่อมั่นให้แก่ประชาชน ภาคธุรกิจ และนักลงทุน อีกทั้งยังเป็นการสนับสนุนนโยบายดิจิทัลของประเทศ ทำให้ประเทศไทยมีมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่ทัดเทียมกับระดับสากล

ผลกระทบที่จะเกิดขึ้น มาตรการนี้จะเพิ่มภาระบางส่วนต่อประชาชนและหน่วยงานของรัฐ แต่จะช่วยลดความเสี่ยงด้านไซเบอร์ในระยะยาว ทำให้บริการของภาครัฐปลอดภัยและน่าเชื่อถือยิ่งขึ้น

#### ๕. ค่าใช้จ่ายและแหล่งที่มา หรือการสูญเสียรายได้

- ไม่มี

#### ๖. ความเห็นหรือความเห็นชอบ/อนุมัติของหน่วยงานที่เกี่ยวข้อง

สกมช. ได้มีการจัดประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ครั้งที่ ๓/๒๕๖๗ เมื่อวันที่ ๓๐ ตุลาคม ๒๕๖๗ โดยมีวาระที่ ๔.๓ เรื่อง แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล และที่ประชุมมีมติ เห็นชอบ แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่ สกมช. เสนอ และมอบหมายให้ สกมช. เสนอแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ให้คณะรัฐมนตรีพิจารณาประกาศให้ทุกหน่วยงานถือปฏิบัติ ต่อไป

#### ๗. ขอกฎหมายและมติคณะรัฐมนตรีที่เกี่ยวข้อง

- ไม่มี

#### ๘. ข้อเสนอของหน่วยงานของรัฐ/คณะกรรมการเจ้าของเรื่อง

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พิจารณาแล้ว ขอเสนอคณะรัฐมนตรีเพื่อโปรดพิจารณาให้ความเห็นชอบ ดังต่อไปนี้

๘.๑ เห็นชอบกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

๘.๒ อนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์  
ให้กับระบบงานของหน่วยงาน ต่อไป

จึงเรียนมาเพื่อโปรดพิจารณานำเสนอคณะรัฐมนตรีต่อไป

ขอแสดงความนับถือ



(นายประเสริฐ จันทรรวงทอง)

รองนายกรัฐมนตรี

ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

โทรศัพท์ ๐ ๒๑๔๒ ๖๘๘๕

ไปรษณีย์อิเล็กทรอนิกส์ : thaicert@ncsa.or.th