ด่วนที่สุด

ที่ นร ๐๕๐๕/ว ๓๔๙

สำนักเลขาธิการคณะรัฐมนตรี
ทำเนียบรัฐบาล กทม. ๑๐๓๐๐

๕ กันยายน ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน รัฐมนตรีว่าการกระทรวงกลาโหม

สิ่งที่ส่งมาด้วย บัญชีสำเนาหนังสือที่ส่งมาด้วย

ด้วยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้เสนอเรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ไปเพื่อดำเนินการ ซึ่งหน่วยงานที่เกี่ยวข้องได้เสนอความเห็นและข้อเสนอแนะไปเพื่อประกอบการพิจารณาของคณะรัฐมนตรีด้วย ความละเอียดปรากฏตามบัญชีสำเนาหนังสือที่ส่งมาด้วยนี้

คณะรัฐมนตรีได้ประชุมปรึกษาเมื่อวันที่ ๒ กันยายน ๒๕๖๘ ลงมติว่า

๑. เห็นชอบและอนุมัติตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ และให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และหน่วยงานที่เกี่ยวข้องรับความเห็นและข้อเสนอแนะของกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักเลขาธิการนายกรัฐมนตรี สำนักงบประมาณ สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ และสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ไปพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

๒. ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจัดให้มีกิจกรรมหรือการดำเนินงานเกี่ยวกับการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ เช่น การให้บริการตรวจค้นหาช่องโหว่หรือการทดสอบเจาะระบบแก่ระบบสารสนเทศก่อนนำไปใช้งานจริงโดยไม่มีค่าใช้จ่าย การเป็นหน่วยงานกลางในการจัดฝึกอบรมผู้พัฒนาระบบและบุคลากรที่เกี่ยวข้อง รวมถึงสนับสนุนการเฝ้าระวังภัยคุกคามทางไซเบอร์ให้แก่ระบบสารสนเทศของหน่วยงานของรัฐทั้งหมด เพื่อป้องกันข้อมูลส่วนบุคคลมิให้เกิดการรั่วไหล

จึงเรียนยืนยันมา

ขอแสดงความนับถือ

(นางณัฐฏ์จารี อนันตศิลป์)
เลขาธิการคณะรัฐมนตรี

กองพัฒนายุทธศาสตร์และติดตามนโยบายพิเศษ
โทร. ๐ ๒๒๘๐ ๙๐๐๐ ต่อ ๑๖๓๒ (วีนัสรินทร์), ๑๕๓๒ (ปัญฑารีย์)
โทรสาร ๐ ๒๒๘๐ ๑๔๔๖
www.soc.go.th
ไปรษณีย์อิเล็กทรอนิกส์ saraban@soc.go.th

บัญชีสำเนาหนังสือที่ส่งมาด้วย

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

๑. สำเนาหนังสือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ด่วนที่สุด ที่ สกมช ๐๘๑๐/๓๕๗๑ ลงวันที่ ๑๖ พฤษภาคม ๒๕๖๘
๒. สำเนาหนังสือกระทรวงกลาโหม ด่วนที่สุด ที่ กห ๐๒๐๗/๑๑๗๔ ลงวันที่ ๑๘ มิถุนายน ๒๕๖๘
๓. สำเนาหนังสือกระทรวงการคลัง ด่วนที่สุด ที่ กค ๐๒๐๒/๑๑๑๒๒ ลงวันที่ ๒๙ สิงหาคม ๒๕๖๘
๔. สำเนาหนังสือกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ ด่วนที่สุด ที่ พม ๐๒๐๙/๑๓๐๒๗ ลงวันที่ ๑๖ กรกฎาคม ๒๕๖๘
๕. สำเนาหนังสือกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ด่วนที่สุด ที่ ดศ ๐๑๐๐.๔/๒๔๘ ลงวันที่ ๒๕ กรกฎาคม ๒๕๖๘
๖. สำเนาหนังสือกระทรวงแรงงาน ด่วนที่สุด ที่ รง ๐๒๐๑.๒/๒๓๒๙ ลงวันที่ ๑๗ กรกฎาคม ๒๕๖๘
๗. สำเนาหนังสือกระทรวงศึกษาธิการ ด่วนที่สุด ที่ ศธ ๐๒๐๒.๒/๑๙๙๙ ลงวันที่ ๑๗ มิถุนายน ๒๕๖๘
๘. สำเนาหนังสือกระทรวงสาธารณสุข ที่ สธ ๐๒๑๒/๒๓๔๐ ลงวันที่ ๒๓ มิถุนายน ๒๕๖๘
๙. สำเนาหนังสือสำนักเลขาธิการนายกรัฐมนตรี ที่ นร ๐๔๐๘/๗๔๕๗ ลงวันที่ ๙ กรกฎาคม ๒๕๖๘
๑๐. สำเนาหนังสือสำนักงบประมาณ ด่วนที่สุด ที่ นร ๐๗๐๘/๖๘๔ ลงวันที่ ๒๙ สิงหาคม ๒๕๖๘
๑๑. สำเนาหนังสือสำนักงานคณะกรรมการกฤษฎีกา ด่วนที่สุด ที่ นร ๐๙๐๙/๘๘ ลงวันที่ ๓๐ พฤษภาคม ๒๕๖๘
๑๒. สำเนาหนังสือสำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ ที่ นร ๑๑๑๖/๒๘๕๓ ลงวันที่ ๑๗ มิถุนายน ๒๕๖๘
๑๓. สำเนาหนังสือสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ด่วนที่สุด ที่ สพร ๒๕๖๘/๑๕๙๐ ลงวันที่ ๒๗ พฤษภาคม ๒๕๖๘

NCS สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ อีเมล saraban@ncsa.or.th

ด่วนที่สุด
ที่ สกมช ๐๘๑๐/ ๓๕๗๑

๑๖ พฤษภาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

สิ่งที่ส่งมาด้วย รายงานการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๓/๒๕๖๗

ด้วยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ขอเสนอ เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล มาเพื่อคณะรัฐมนตรีพิจารณาเห็นชอบ โดยเรื่องนี้เข้าข่ายที่จะให้นำเสนอคณะรัฐมนตรีได้ตามพระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๔ (๑)

ทั้งนี้ เรื่องดังกล่าวมีรายละเอียด ดังนี้

๑. <u>เหตุผลความจำเป็นที่ต้องเสนอคณะรัฐมนตรี</u>

การเสนอกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล มีความจำเป็นต้องเสนอคณะรัฐมนตรีเพื่อพิจารณาและให้ความเห็นชอบ เนื่องจากเป็นการดำเนินการตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๐) ซึ่งกำหนดให้ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่เสนอแนะและให้ความเห็นต่อ คณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

นอกจากนี้ มาตรา ๒๒ (๕) และ (๖) ของพระราชบัญญัติฉบับเดียวกัน ได้กำหนดให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงเฝ้าระวัง ติดตาม วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ ซึ่งเป็นหน้าที่สำคัญที่เกี่ยวข้องโดยตรงกับการดำเนินการตามกรอบแนวทางที่เสนอ

ดังนั้น เรื่องนี้จึงเข้าข่ายเรื่องที่ต้องเสนอคณะรัฐมนตรีตาม พระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๔ (๑) เรื่องที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของคณะรัฐมนตรีหรือให้ต้องเสนอคณะรัฐมนตรี

๒. <u>ความเร่งด่วนของเรื่อง</u>

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีความจำเป็นที่จะต้องเสนอขอความเห็นชอบและอนุมัติในต่อกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐจากคณะรัฐมนตรี เนื่องจากปัจจุบันมีการรั่วไหลของข้อมูลส่วนบุคคลเป็นจำนวนมาก จึงขอความกรุณาเสนอเรื่องนี้ต่อคณะรัฐมนตรีภายในเดือนมิถุนายน ๒๕๖๘

/๓. <u>สาระ</u>...

๓. <u>สาระสำคัญและข้อเท็จจริง</u>

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 ตลอดจนกำหนดให้มีการกำกับดูและติดตาม รวมทั้งการทดสอบความปลอดภัยระบบเป็นประจำ ทั้งในช่วงการพัฒนาและก่อนการใช้งานจริงเพื่อค้นหาช่องโหว่และแก้ไขทันที

๒) หน่วยงานควรจัดการอบรมสำหรับผู้พัฒนาและบุคลากรที่เกี่ยวข้องในเรื่องการออกแบบและพัฒนาระบบให้ปลอดภัย พร้อมสร้างความรับรู้ในเรื่องภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น

๓) จัดให้มีการตรวจสอบและประเมินผลการทำงานของระบบอย่างสม่ำเสมอ รวมถึงการตรวจสอบความสอดคล้องกับมาตรฐานความปลอดภัยที่กำหนด

๔) กำหนดให้มีการระบุเงื่อนไขด้านความปลอดภัยในสัญญาว่าจ้างผู้พัฒนา โดยเน้นความรับผิดชอบต่อปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นจากการพัฒนา

๕) จัดให้มีกลไกการเฝ้าระวังเพื่อแจ้งเตือนและตอบสนองต่อการโจมตีหรือช่องโหว่ที่เกิดขึ้นอย่างรวดเร็ว รวมถึงการมีแผนรับมือเมื่อเกิดเหตุการณ์ความปลอดภัยไซเบอร์

๖) สนับสนุนการปรับปรุงระบบให้ทันสมัยอยู่เสมอ โดยอัปเดตซอฟต์แวร์และแพตช์ด้านความปลอดภัยเมื่อมีช่องโหว่ถูกค้นพบ

๗) หากมีระบบงานที่ไม่ได้ใช้งาน ควรมีการปิดระบบเพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลได้

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

/ทั้งนี้ ...

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

๔. <u>ประโยชน์และผลกระทบ</u>

การดำเนินการตามกรอบแนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ จะช่วยยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในภาครัฐอย่างเป็นระบบ ส่งผลให้ระบบดิจิทัลของรัฐมีความมั่นคงปลอดภัยมากยิ่งขึ้น เพิ่มความเชื่อมั่นให้แก่ประชาชน ภาคธุรกิจ และนักลงทุน อีกทั้งยังเป็นการสนับสนุนนโยบายดิจิทัลของประเทศ ทำให้ประเทศไทยมีมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่ทัดเทียมกับระดับสากล

ผลกระทบที่จะเกิดขึ้น มาตรการนี้จะเพิ่มภาระบางส่วนต่อประชาชนและหน่วยงานของรัฐ แต่จะช่วยลดความเสี่ยงด้านไซเบอร์ในระยะยาว ทำให้บริการของภาครัฐปลอดภัยและน่าเชื่อถือยิ่งขึ้น

๕. <u>ค่าใช้จ่ายและแหล่งที่มา หรือการสูญเสียรายได้</u>

- ไม่มี

๖. <u>ความเห็นหรือความเห็นชอบ/อนุมัติของหน่วยงานที่เกี่ยวข้อง</u>

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. <u>ข้อกฎหมายและมติคณะรัฐมนตรีที่เกี่ยวข้อง</u>

- ไม่มี

๘. <u>ข้อเสนอของหน่วยงานของรัฐ/คณะกรรมการเจ้าของเรื่อง</u>

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พิจารณาแล้ว ขอเสนอคณะรัฐมนตรีเพื่อโปรดพิจารณาให้ความเห็นชอบ ดังต่อไปนี้

๘.๑ เห็นชอบกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

/๘.๒ อนุมัติ...

๘.๒ อนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงาน ต่อไป

จึงเรียนมาเพื่อโปรดพิจารณานำเสนอคณะรัฐมนตรีต่อไป

ขอแสดงความนับถือ

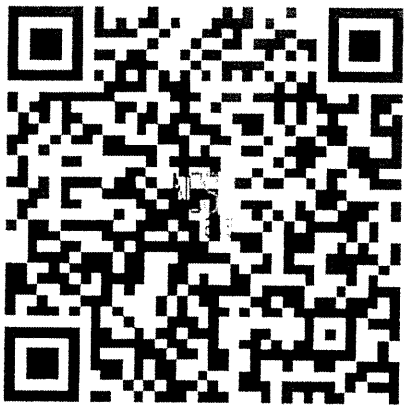
(นายประเสริฐ จันทรรวงทอง)
รองนายกรัฐมนตรี
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
โทรศัพท์ ๐ ๒๑๔๒ ๖๘๘๕
ไปรษณีย์อิเล็กทรอนิกส์ : thaicert@ncsa.or.th

สำเนาถูกต้อง

ปัญฑารีย์ ดีประเสริฐไชย

(นางสาวปัญฑารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
- 2 ก.ย. 2568



ด่วนที่สุด
ที่ กห ๐๒๐๗/ว ๒๑๔

กระทรวงกลาโหม
ถนนสนามไชย เขตพระนคร
กรุงเทพมหานคร ๑๐๒๐๐

๑๙ มิถุนายน ๒๕๖๘

เรื่อง เสนอความเห็นเรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามที่สำนักเลขาธิการคณะรัฐมนตรี ขอให้กระทรวงกลาโหม พิจารณาเสนอความเห็นในส่วนที่เกี่ยวข้อง เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เสนอ เพื่อบรรจุเข้าระเบียบวาระการพิจารณาของคณะรัฐมนตรี ความละเอียดแจ้งแล้วนั้น

กระทรวงกลาโหม พิจารณาแล้วมีความเห็นว่า กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล เป็นการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และนโยบายของรัฐบาลในการปฏิรูประบบราชการให้มีความทันสมัยสู่การเป็นรัฐบาลดิจิทัล (Digital Government) รวมทั้งมุ่งเน้นการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ ควบคู่ไปกับการยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลอย่างเป็นระบบ เพื่อลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในภาครัฐ อันจะส่งผลให้ระบบดิจิทัลของรัฐมีความมั่นคงปลอดภัยได้มาตรฐานสากลมากขึ้น

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายภูมิธรรม เวชยชัย)
รัฐมนตรีว่าการกระทรวงกลาโหม

สำนักงานปลัดกระทรวงกลาโหม
สำนักนโยบายและแผนกลาโหม
โทร. ๐ ๒๒๒๒ ๔๓๖๙
โทรสาร ๐ ๒๒๒๒ ๔๓๖๘

สำเนาถูกต้อง

บัญฑารีย์ ดีประเสริฐไชย

(นางสาวบัญฑารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
- 2 ก.ย. 2568

ด่วนที่สุด
ที่ กค ๐๒๐๒/๗๗๐๒๖

กระทรวงการคลัง
ถนนพระรามที่ ๖
กรุงเทพฯ ๑๐๔๐๐

๒๕ สิงหาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรีขอให้กระทรวงการคลังเสนอความเห็นในส่วนที่เกี่ยวข้องต่อกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ เพื่อประกอบการพิจารณาของคณะรัฐมนตรีโดยด่วน ความละเอียดแจ้งแล้ว นั้น

กระทรวงการคลังพิจารณาแล้ว ขอเรียนว่า กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ได้กำหนดแนวทางการดำเนินการตามมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันจะส่งผลดีและเป็นประโยชน์ต่อหน่วยงานภาครัฐในการปฏิบัติการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งจะช่วยยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลในภาครัฐอย่างเป็นระบบและมีความมั่นคงปลอดภัยมากยิ่งขึ้น จึงไม่ขัดข้องในหลักการของกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายพิชัย ชุณหวชิร)
รัฐมนตรีว่าการกระทรวงการคลัง

สำนักงานปลัดกระทรวงการคลัง
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทรศัพท์ ๐ ๒๑๒๖ ๕๙๐๐ ต่อ ๓๐๓๐๑
โทรสาร ๐ ๒๒๗๓ ๙๗๙๐

สำเนาถูกต้อง
ปัญฑารีย์ ดีประเสริฐไชย
(นางสาวปัญฑารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
-2 ก.ย. 2568

NCS สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ อีเมล saraban@ncsa.or.th

ด่วนที่สุด
ที่ สกมช ๐๘๑๐/ ๓๕๗๑

๑๖ พฤษภาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

สิ่งที่ส่งมาด้วย รายงานการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๓/๒๕๖๗

ด้วยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ขอเสนอ เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล มาเพื่อคณะรัฐมนตรีพิจารณาเห็นชอบ โดยเรื่องนี้เข้าข่ายที่จะให้นำเสนอคณะรัฐมนตรีได้ตามพระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๔ (๑)

ทั้งนี้ เรื่องดังกล่าวมีรายละเอียด ดังนี้

๑. <u>เหตุผลความจำเป็นที่ต้องเสนอคณะรัฐมนตรี</u>

การเสนอกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล มีความจำเป็นต้องเสนอคณะรัฐมนตรีเพื่อพิจารณาและให้ความเห็นชอบ เนื่องจากเป็นการดำเนินการตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๐) ซึ่งกำหนดให้ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่เสนอแนะและให้ความเห็นต่อ คณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

นอกจากนี้ มาตรา (๕) และ (๖) ของพระราชบัญญัติฉบับเดียวกัน ได้กำหนดให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติมีหน้าที่ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงเฝ้าระวัง ติดตาม วิเคราะห์ และแจ้งเตือนภัยคุกคามทางไซเบอร์ ซึ่งเป็นหน้าที่สำคัญที่เกี่ยวข้องโดยตรงกับการดำเนินการตามกรอบแนวทางที่เสนอ

ดังนั้น เรื่องนี้จึงเข้าข่ายเรื่องที่ต้องเสนอคณะรัฐมนตรีตาม พระราชกฤษฎีกาว่าด้วยการเสนอเรื่องและการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๔ (๑) ซึ่งกำหนดให้เรื่องที่เกี่ยวข้องกับนโยบายความมั่นคง และการบริหารราชการแผ่นดิน ต้องนำเสนอคณะรัฐมนตรีพิจารณาเห็นชอบ

๒. <u>ความเร่งด่วนของเรื่อง</u>

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีความจำเป็นที่จะต้องเสนอขอความเห็นชอบและอนุมัติในต่อกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐจากคณะรัฐมนตรี เนื่องจากปัจจุบันมีการรั่วไหลของข้อมูลส่วนบุคคลเป็นจำนวนมาก จึงขอความกรุณาเสนอเรื่องนี้ต่อคณะรัฐมนตรีภายในเดือนมิถุนายน ๒๕๖๘

/๓. สาระ...

๓. <u>สาระสำคัญและข้อเท็จจริง</u>

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้มีการจัดประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ครั้งที่ ๓/๒๕๖๗ เมื่อวันที่ ๓๐ ตุลาคม ๒๕๖๗ โดยมีวาระที่ ๔.๓ เรื่อง แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้ดำเนินการติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อให้ความช่วยเหลือ 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 ตลอดจนกำหนดให้มีการกำกับดูและติดตาม รวมทั้งการทดสอบความปลอดภัยระบบเป็นประจำ ทั้งในช่วงการพัฒนาและก่อนการใช้งานจริงเพื่อค้นหาช่องโหว่และแก้ไขทันที

๒) หน่วยงานควรจัดการอบรมสำหรับผู้พัฒนาและบุคลากรที่เกี่ยวข้องในเรื่องการออกแบบและพัฒนาระบบให้ปลอดภัย พร้อมสร้างความรับรู้ในเรื่องภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น

๓) จัดให้มีการตรวจสอบและประเมินผลการทำงานของระบบอย่างสม่ำเสมอ รวมถึงการตรวจสอบความสอดคล้องกับมาตรฐานความปลอดภัยที่กำหนด

๔) กำหนดให้มีการระบุเงื่อนไขด้านความปลอดภัยในสัญญาว่าจ้างผู้พัฒนา โดยเน้นความรับผิดชอบต่อปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นจากการพัฒนา

๕) จัดให้มีกลไกการเฝ้าระวังเพื่อแจ้งเตือนและตอบสนองต่อการโจมตีหรือช่องโหว่ที่เกิดขึ้นอย่างรวดเร็ว รวมถึงการมีแผนรับมือเมื่อเกิดเหตุการณ์ความปลอดภัยไซเบอร์

๖) สนับสนุนการปรับปรุงระบบให้ทันสมัยอยู่เสมอ โดยอัปเดตซอฟต์แวร์และแพตช์ด้านความปลอดภัยเมื่อมีช่องโหว่ถูกค้นพบ

๗) หากมีระบบงานที่ไม่ได้ใช้งาน ควรมีการปิดระบบเพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลได้

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

/ทั้งนี้ ...

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

๔. <u>ประโยชน์และผลกระทบ</u>

การดำเนินการตามกรอบแนวทางการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ จะช่วยยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในภาครัฐอย่างเป็นระบบ ส่งผลให้ระบบดิจิทัลของรัฐมีความมั่นคงปลอดภัยมากยิ่งขึ้น เพิ่มความเชื่อมั่นให้แก่ประชาชน ภาคธุรกิจ และนักลงทุน อีกทั้งยังเป็นการสนับสนุนนโยบายดิจิทัลของประเทศ ทำให้ประเทศไทยมีมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่ทัดเทียมกับระดับสากล

ผลกระทบที่จะเกิดขึ้น มาตรการนี้จะเพิ่มภาระบางส่วนต่อประชาชนและหน่วยงานของรัฐ แต่จะช่วยลดความเสี่ยงด้านไซเบอร์ในระยะยาว ทำให้บริการของภาครัฐปลอดภัยและน่าเชื่อถือยิ่งขึ้น

๕. <u>ค่าใช้จ่ายและแหล่งที่มา หรือการสูญเสียรายได้</u>

- ไม่มี

๖. <u>ความเห็นหรือความเห็นชอบ/อนุมัติของหน่วยงานที่เกี่ยวข้อง</u>

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. <u>ข้อกฎหมายและมติคณะรัฐมนตรีที่เกี่ยวข้อง</u>

- ไม่มี

๘. <u>ข้อเสนอของหน่วยงานของรัฐ/คณะกรรมการเจ้าของเรื่อง</u>

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พิจารณาแล้ว ขอเสนอคณะรัฐมนตรีเพื่อโปรดพิจารณาให้ความเห็นชอบ ดังต่อไปนี้

๘.๑ เห็นชอบกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

/๘.๒ อนุมัติ...

๘.๒ อนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงาน ต่อไป

จึงเรียนมาเพื่อโปรดพิจารณานำเสนอคณะรัฐมนตรีต่อไป

ขอแสดงความนับถือ

(นายประเสริฐ จันทรรวงทอง)
รองนายกรัฐมนตรี
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
โทรศัพท์ ๐ ๒๑๔๒ ๖๘๘๕
ไปรษณีย์อิเล็กทรอนิกส์ : thaicert@ncsa.or.th

ด่วนที่สุด
ที่ พม ๐๒๐๙/๑๓๐๖๗

กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
๑๐๓๔ ถนนกรุงเกษม แขวงคลองมหานาค
เขตป้อมปราบศัตรูพ่าย กทม. ๑๐๑๐๐

๑๖ กรกฎาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

สิ่งที่ส่งมาด้วย ความเห็นประกอบการพิจารณาของคณะรัฐมนตรี จำนวน ๑ ชุด

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรี แจ้งขอให้กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เสนอความเห็นต่อกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ เพื่อประกอบการพิจารณาของคณะรัฐมนตรี ความละเอียดแจ้งแล้ว นั้น

กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เห็นด้วยในหลักการตามกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ซึ่งเป็นการยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลที่เหมาะสมกับบริบทของภาครัฐที่มีการจัดเก็บข้อมูลส่วนบุคคลจำนวนมาก โดยเฉพาะข้อมูลที่มีความอ่อนไหว อาทิ ข้อมูลสุขภาพ ข้อมูลสวัสดิการ ข้อมูลกลุ่มเปราะบาง ฯลฯ อย่างไรก็ตาม การนำกรอบแนวทางดังกล่าวไปปฏิบัติในหน่วยงานของรัฐจำเป็นต้องได้รับการสนับสนุนตั้งแต่ระดับนโยบาย การจัดสรรงบประมาณ และการเสริมสร้างความเข้าใจให้แก่เจ้าหน้าที่ของรัฐ เพื่อให้บุคลากรทุกระดับมีความตระหนักต่อการป้องกันและลดความเสี่ยงภัยคุกคามทางไซเบอร์ เพื่อให้สามารถดำเนินงานตามภารกิจได้อย่างรัดกุม โปร่งใส และเป็นไปตามหลักธรรมาภิบาลทางดิจิทัล (Digital Governance Principles) และส่งผลให้งานบริการของภาครัฐมีความมั่นคงปลอดภัยยิ่งขึ้น ทั้งนี้ กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ มีข้อเสนอแนะเพิ่มเติม เพื่อสนับสนุนการดำเนินการตามกรอบแนวทางดังกล่าวในการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลอย่างเป็นระบบและมีประสิทธิภาพ รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายวราวุธ ศิลปอาชา)
รัฐมนตรีว่าการกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

สำเนาถูกต้อง
ปัญฑารีย์ ดีประเสริฐไชย
(นางสาวปัญฑารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
- 2 ก.ค. 2568

สำนักงานปลัดกระทรวงฯ
กองยุทธศาสตร์และแผนงาน
โทร. ๐ ๒๖๕๙ ๖๔๙๔
โทรสาร ๐ ๒๖๕๙ ๖๔๙๘

ความเห็นประกอบการพิจารณาของคณะรัฐมนตรี
ของกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
ต่อ
กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ
สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ เห็นด้วยในหลักการตามกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ซึ่งเป็นการยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลที่เหมาะสมกับบริบทของภาครัฐที่มีการจัดเก็บข้อมูลส่วนบุคคลจำนวนมาก โดยเฉพาะข้อมูลที่มีความอ่อนไหว อาทิ ข้อมูลสุขภาพ ข้อมูลสวัสดิการ ข้อมูลกลุ่มเปราะบาง ฯลฯ อย่างไรก็ตาม การนำกรอบแนวทางดังกล่าวไปปฏิบัติในหน่วยงานของรัฐ จำเป็นต้องได้รับการสนับสนุนตั้งแต่ระดับนโยบาย การจัดสรรงบประมาณ และการเสริมสร้างความเข้าใจให้แก่เจ้าหน้าที่ของรัฐ เพื่อให้บุคลากรทุกระดับมีความตระหนักต่อการป้องกันและลดความเสี่ยงภัยคุกคามทางไซเบอร์ เพื่อให้สามารถดำเนินงานตามภารกิจได้อย่างรัดกุม โปร่งใส และเป็นไปตามหลักธรรมาภิบาลทางดิจิทัล (Digital Governance Principles) และส่งผลให้งานบริการของภาครัฐมีความมั่นคงปลอดภัยยิ่งขึ้น ทั้งนี้ กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ มีข้อเสนอแนะเพิ่มเติม เพื่อสนับสนุนการดำเนินการตามกรอบแนวทางดังกล่าวในการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลอย่างเป็นระบบและมีประสิทธิภาพ ดังนี้

๑. **การกำหนดขอบเขตของงานพัฒนาระบบหน่วยงาน** ควรกำหนดให้มีการประเมินผลกระทบด้านความเป็นส่วนตัว (Privacy Impact Assessment : PIA) ก่อนเริ่มพัฒนาระบบที่มีการจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล เพื่อประเมินประเภทของข้อมูลที่จัดเก็บ สิทธิ์การเข้าถึง และความเสี่ยงที่อาจเกิดขึ้น พร้อมทั้งควรกำหนดให้ใช้ข้อมูลจำลองแทนข้อมูลจริงในการทดสอบ และลบออกภายใน ๓ วันหลังจบแต่ละรอบการทดสอบ เพื่อป้องกันความเสี่ยงจากการตกค้างของข้อมูล นอกจากนี้ ควรเพิ่มกระบวนการตรวจสอบความปลอดภัยของรหัสต้นทาง (Source code) และการสแกนช่องโหว่ (Static Application Security Testing : SAST) ก่อนนำระบบขึ้นใช้งานจริง โดยต้องไม่มีช่องโหว่ในระดับที่มีความรุนแรงสูงสุดตามมาตรฐาน Common Vulnerability Scoring System หรือ CVSS และกำหนดให้ขอบเขตของงาน (Terms of Reference : TOR) ของผู้พัฒนาต้องผ่านการรับรองมาตรฐานด้านความมั่นคงปลอดภัย อาทิ ISO/IEC 27001 NIST CSF ฯลฯ

๒. **การอบรมและสร้างความรู้ความเข้าใจแก่บุคลากร** ควรจัดอบรมเฉพาะด้านให้แก่ผู้พัฒนาในเรื่อง แนวทางการพัฒนาซอฟต์แวร์ที่มีความทนทานต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี (Secure Coding) โดยครอบคลุมเนื้อหาหลัก เช่น การตรวจสอบข้อมูลนำเข้า การออกแบบการยืนยันตัวตนที่ปลอดภัย เป็นต้น พร้อมมีแบบทดสอบหลังอบรม และออกใบรับรองที่มีการต่ออายุทุกปี เพื่อรักษามาตรฐานวิชาชีพอย่างต่อเนื่อง สำหรับบุคลากรทั่วไปควรได้รับการอบรมเรื่อง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) เพื่อให้เข้าใจบทบาทหน้าที่ของตนเอง การขอความยินยอม และสิทธิของเจ้าของข้อมูล

๓. **การตรวจสอบและประเมินผลระบบ** ควรกำหนดให้มีการประเมินความปลอดภัยของระบบอย่างสม่ำเสมอ โดยเฉพาะระบบที่มีความเสี่ยงสูง เช่น ระบบฐานข้อมูลประชาชน เป็นต้น ซึ่งควรให้มีการประเมินอย่างน้อยเป็นรายไตรมาส ส่วนระบบทั่วไปควรประเมินทุก ๖ เดือน และควรกำหนดเกณฑ์การยอมรับความเสี่ยง (Risk Acceptance Criteria) อย่างชัดเจน เช่น ไม่อนุญาตให้นำระบบที่มีช่องโหว่ระดับที่มีความรุนแรงสูงสุด (CVSS ≥ 9.0) ไปใช้งานจริงในระบบ Production

๔. การกำหนด...

๔. **การกำหนดเงื่อนไขในสัญญาว่าจ้างผู้พัฒนาระบบ** ควรกำหนดเงื่อนไขด้านความมั่นคงปลอดภัยในสัญญาว่าจ้างอย่างชัดเจน รวมถึงบทลงโทษในกรณีเกิดการรั่วไหลของข้อมูล เช่น ค่าปรับต่อรายต่อเหตุการณ์ เป็นต้น เพื่อสร้างแรงจูงใจให้เกิดความรับผิดชอบต่อข้อมูลภาครัฐ นอกจากนี้ ผู้รับจ้างควรมีประกันภัยด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Liability Insurance) เพื่อรับมือกับความเสียหายที่อาจเกิดขึ้น และควรระบุสิทธิของหน่วยงานในการตรวจสอบกระบวนการพัฒนา (Right to Audit)

๕. **การใช้งานระบบคลาวด์อย่างมั่นคงปลอดภัย** ซึ่งนอกจากการปฏิบัติตามมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ ซึ่งสอดคล้องกับนโยบาย Cloud First Policy แล้ว ก่อนย้ายข้อมูลขึ้นระบบคลาวด์ ควรมีการประเมินความเสี่ยง (Cloud Security Assessment) และจัดให้มีระบบติดตามและตรวจสอบการใช้งานระบบคลาวด์อย่างต่อเนื่อง พร้อมทั้งกำหนดข้อกำหนดที่ตั้งข้อมูล (Data Residency Requirements) สำหรับข้อมูลที่อ่อนไหว อาทิ ข้อมูลสุขภาพ ข้อมูลสวัสดิการ ฯลฯ ให้จัดเก็บภายในประเทศหรือในเขตเศรษฐกิจที่มีข้อตกลงร่วมกับประเทศไทย

๖. **การจัดการข้อมูลส่วนบุคคลในเชิงระบบ** ควรจัดทำแผนภาพแสดงการไหลของข้อมูล (Data Flow Mapping) เพื่อให้เข้าใจว่าข้อมูลไหลไปถึงผู้ใดบ้าง และบุคคลระดับใดมีสิทธิ์เข้าถึงหรือรับผิดชอบข้อมูลในแต่ละช่วง นอกจากนี้ ควรกำหนดนโยบายการเก็บข้อมูลให้น้อยที่สุดเท่าที่จำเป็น (Data Minimization) และกำหนดระยะเวลาเก็บข้อมูลที่ชัดเจน (Data Retention) เพื่อลดความเสี่ยงและสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) อีกทั้งควรมีกระบวนการที่รองรับการใช้สิทธิ์ของเจ้าของข้อมูล (Data Subject Rights Management) อาทิ การขอแก้ไขข้อมูล ฯลฯ ได้อย่างสะดวกและปลอดภัย

ด่วนที่สุด

ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔

สำนักเลขาธิการคณะรัฐมนตรี
ทำเนียบรัฐบาล กทม. ๑๐๓๐๐

๒๐ พฤษภาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน รัฐมนตรีว่าการกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

สิ่งที่ส่งมาด้วย สำเนาหนังสือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ด่วนที่สุด ที่ สกมช ๐๘๑๐/๓๕๗๑ ลงวันที่ ๑๖ พฤษภาคม ๒๕๖๘

ด้วยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้เสนอเรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ไปเพื่อดำเนินการ ความละเอียดปรากฏตามสำเนาหนังสือที่ส่งมาด้วยนี้

จึงเรียนมาเพื่อโปรดเสนอความเห็นในส่วนที่เกี่ยวข้องเพื่อประกอบการพิจารณาของคณะรัฐมนตรีโดยด่วนด้วย จะขอบคุณยิ่ง

ขอแสดงความนับถือ

ที่ พม ๐๑๐๑/ ๑๐๐๓

- มอบ ปพม. พิจารณาดำเนินการ

ภิวทอง สุวรรณรัตน์

(นางสาวภิวทอง สุวรรณรัตน์)
ผู้อำนวยการกองวิเคราะห์เรื่องเสนอคณะรัฐมนตรี ปฏิบัติราชการแทน
เลขาธิการคณะรัฐมนตรี

(นายวราวุธ ศิลปอาชา)
รมว.พม.
๒๗ พ.ค. ๖๘

กองวิเคราะห์เรื่องเสนอคณะรัฐมนตรี
โทร. ๐ ๒๒๘๐ ๔๐๐๐ ต่อ ๑๖๓๒ , ๐๘ ๕๑๔๐ ๓๖๖๕ (วีนัสรินทร์)
โทรสาร ๐ ๒๒๘๐ ๔๐๖๔
ไปรษณีย์อิเล็กทรอนิกส์ : saraban@soc.go.th

มอบหมาย รมช. ปภ.สานสัมพันธ์

(นางจตุพร โรจนพานิช)
รองปลัดกระทรวง รักษาราชการแทน
ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
๒๘ พ.ค. ๒๕๖๘

ด่วนที่สุด

ที่ ดศ ๐๑๐๐.๔/๒๔๘

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษาฯ
อาคารซี ซอยแจ้งวัฒนะ ๗ ถนนแจ้งวัฒนะ
เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

๒๕ กรกฎาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรีขอให้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเสนอความเห็นในส่วนที่เกี่ยวข้องเรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล เพื่อประกอบการพิจารณาของคณะรัฐมนตรี ความละเอียดแจ้งแล้ว นั้น

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาแล้ว ไม่มีข้อขัดข้องในหลักการต่อกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ เนื่องจากเป็นการกำหนดแนวปฏิบัติสำคัญเพื่อยกระดับมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ในการป้องกันการรั่วไหลของข้อมูลส่วนบุคคลของหน่วยงานของรัฐอย่างเป็นระบบ ซึ่งจะมีส่วนสำคัญในการเสริมสร้างเสถียรภาพของระบบดิจิทัลของหน่วยงานของรัฐและความเชื่อมั่นของประชาชนในภาพรวม ทั้งนี้ กรอบแนวทางดังกล่าวยังมีความสอดคล้องกับมาตรฐานสากลและสนับสนุนการดำเนินงานตามนโยบายการใช้คลาวด์เป็นหลักของรัฐบาล อย่างไรก็ดี เพื่อให้การนำกรอบแนวทางดังกล่าวไปสู่การปฏิบัติอย่างเคร่งครัดและเป็นรูปธรรม กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเห็นควรให้มีการกำหนดกลไกในการติดตาม ตรวจสอบและประเมินผลอย่างต่อเนื่อง เพื่อนำมาปรับปรุงและพัฒนาแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ให้สามารถรับมือกับสถานการณ์และภัยคุกคามที่เปลี่ยนแปลงอย่างรวดเร็ว อันจะนำไปสู่ระบบดิจิทัลของหน่วยงานของรัฐที่มีความมั่นคงปลอดภัย และสร้างความเชื่อมั่นให้กับประชาชนอย่างแท้จริง

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายประเสริฐ จันทรรวงทอง)
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำเนาถูกต้อง

ปัญฑารีย์ ดีประเสริฐไชย
(นางสาวปัญฑารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
- 2 ก.ย. 2568

สำนักงานปลัดกระทรวง
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทรศัพท์ ๐ ๒๑๔๑ ๖๙๐๙
ไปรษณีย์อิเล็กทรอนิกส์ saraban@mdes.go.th

ด่วนที่สุด
ที่ รง ๐๒๐๑.๒/๒๓๒๙

กระทรวงแรงงาน
ถนนมิตรไมตรี ดินแดง
กรุงเทพมหานคร ๑๐๔๐๐

๑๗ กรกฎาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรีขอให้กระทรวงแรงงานพิจารณาเสนอความเห็นในส่วนที่เกี่ยวข้อง เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อประกอบการพิจารณาของคณะรัฐมนตรี ความละเอียดแจ้งแล้ว นั้น

กระทรวงแรงงานพิจารณาแล้ว ไม่ขัดข้องต่อกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ เนื่องจากกรอบแนวทางดังกล่าวจะช่วยยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในภาครัฐอย่างเป็นระบบ ทำให้บริการของภาครัฐปลอดภัยและน่าเชื่อถือยิ่งขึ้น

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นายพงศ์กวิน จึงรุ่งเรืองกิจ)
รัฐมนตรีว่าการกระทรวงแรงงาน

สำนักงานปลัดกระทรวง
กองกลาง
โทรศัพท์ ๐ ๒๒๓๒ ๑๑๕๗
ไปรษณีย์อิเล็กทรอนิกส์ saraban.mol@mol.mail.go.th

สำเนาถูกต้อง
ปัญทารีย์ ดีประเสริฐไชย
(นางสาวปัญทารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
- 2 ก.ย. 2568

ด่วนที่สุด

ที่ ศธ ๐๒๐๒.๒/ ๑๕๕๕

กระทรวงศึกษาธิการ
กทม. ๑๐๓๐๐

๑๗ มิถุนายน ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรีขอให้กระทรวงศึกษาธิการเสนอความเห็นในส่วนที่เกี่ยวข้องเพื่อประกอบการพิจารณาของคณะรัฐมนตรี เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ความละเอียดแจ้งแล้ว นั้น

กระทรวงศึกษาธิการ พิจารณาแล้ว เพื่อเป็นการยกระดับมาตรการป้องกันข้อมูลส่วนบุคคลและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อย่างเป็นระบบ ส่งผลให้ระบบดิจิทัลของหน่วยงานมีความมั่นคงปลอดภัยมากยิ่งขึ้น จึงเห็นด้วยกับกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล และดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงานต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

พลตำรวจเอก

(เพิ่มพูน ชิดชอบ)
รัฐมนตรีว่าการกระทรวงศึกษาธิการ

สำนักงานปลัดกระทรวง
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทรศัพท์ ๐ ๒๒๘๑ ๒๗๑๒
โทรสาร ๐ ๒๒๘๑ ๘๒๑๘
E-mail: sarabun_bict@moe.go.th

สำเนาถูกต้อง
ปัญฑารีย์ ดีประเสริฐไชย
(นางสาวปัญฑารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
- 2 ก.ย. 2568

"เรียนดี มีความสุข"

ที่ สธ ๐๒๑๒/๒๓๔๐

กระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๒๓ มิถุนายน ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรี ขอให้กระทรวงสาธารณสุขให้ความเห็นในส่วนที่เกี่ยวข้อง เพื่อประกอบการพิจารณาของคณะรัฐมนตรี ประเด็นความเห็น เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ความละเอียดแจ้งแล้ว นั้น

กระทรวงสาธารณสุข พิจารณาแล้วมีความเห็นว่าเพื่อให้หน่วยงานภายใต้สังกัดกระทรวงสาธารณสุขซึ่งมีการเก็บ รวบรวม ใช้ และประมวลผลข้อมูลสุขภาพส่วนบุคคล มีแนวทางปฏิบัติในการสร้างความมั่นคงปลอดภัยไซเบอร์สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลอย่างเป็นรูปธรรมและเป็นไปตามมาตรฐานสากล อาทิ ISO/IEC 27001 หรือ NIST Cyber Security Framework จึงเห็นชอบในหลักการของกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ

จึงเรียนมาเพื่อโปรดพิจารณาและดำเนินการต่อไปด้วย จะเป็นพระคุณ

ขอแสดงความนับถือ

(นายสมศักดิ์ เทพสุทิน)
รัฐมนตรีว่าการกระทรวงสาธารณสุข

สำนักงานปลัดกระทรวงสาธารณสุข
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทร. ๐ ๒๕๙๐ ๑๒๑๓
ไปรษณีย์อิเล็กทรอนิกส์ saraban0212@moph.go.th

สำเนาถูกต้อง
ปัญฑารีย์ ดีประเสริฐไชย
(นางสาวปัญฑารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
- 2 ก.ย. 2568

ที่ นร ๐๔๐๘/ ๗๔๕๗

สำนักเลขาธิการนายกรัฐมนตรี
ทำเนียบรัฐบาล กทม. ๑๐๓๐๐

๙ กรกฎาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง ขอให้สำนักเลขาธิการนายกรัฐมนตรีเสนอความเห็นเพื่อประกอบการพิจารณาของคณะรัฐมนตรี เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ ความละเอียดแจ้งแล้ว นั้น

สำนักเลขาธิการนายกรัฐมนตรีพิจารณาแล้ว เห็นด้วยในหลักการข้อเสนอของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เนื่องจากเป็นการยกระดับมาตรการป้องกันการรั่วไหลของข้อมูลส่วนบุคคลของหน่วยงานภาครัฐ ซึ่งเป็นภัยคุกคามที่ส่งผลกระทบต่อความเชื่อมั่นและความมั่นคงของประเทศ เพื่อให้มีมาตรฐานทัดเทียมกับระดับสากล ส่งผลให้บริการภาครัฐปลอดภัยและน่าเชื่อถือยิ่งขึ้น โดยมีข้อเสนอสำหรับประกอบการดำเนินการเพิ่มเติม ดังนี้

๑. ควรมีการจัดทำทะเบียนรายชื่อผู้รับจ้างที่มีคุณสมบัติและความเชี่ยวชาญด้านความปลอดภัยไซเบอร์ที่เชื่อถือได้ เพื่อเป็นแหล่งข้อมูลให้หน่วยงานภาครัฐใช้ประกอบการพิจารณาเลือกผู้รับจ้างพัฒนาระบบ ทั้งนี้ เพื่อเป็นการกำกับดูแลและตรวจสอบผู้รับจ้างให้มีการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่กำหนดอย่างเคร่งครัด

๒. ควรมีกลไกและเครื่องมือ (Toolkit) ให้หน่วยงานของรัฐสามารถนำไปใช้ในการตรวจสอบความมั่นคงปลอดภัยของระบบอย่างต่อเนื่อง (Regular Security Audit) เพื่อประเมินจุดอ่อน/จุดเสี่ยง และหาทางปรับปรุงแก้ไขได้ทันท่วงที รวมทั้งควรมีระบบสำหรับแลกเปลี่ยนข้อมูลและเผยแพร่บทเรียนจากเหตุการณ์ความปลอดภัยไซเบอร์ เพื่อแจ้งเตือนและเตรียมพร้อมสำหรับป้องกันและจัดการกับภัยคุกคามที่คล้ายคลึงกัน

/๓. ควรส่งเสริม...

๓. ควรส่งเสริมให้หน่วยงานของรัฐสร้างวัฒนธรรมความปลอดภัยไซเบอร์ โดยในระดับองค์กรควรมีการกำหนดเป็นตัวชี้วัด (KPI) ให้ทุกหน่วยงาน โดยเฉพาะหน่วยงานที่ได้รับการประเมินตรวจสอบว่ามีความเสี่ยงต่อภัยคุกคามด้านไซเบอร์และการรั่วไหลของข้อมูลส่วนบุคคลต้องมีการจัดทำแผนรับมือเมื่อเกิดเหตุการณ์ความปลอดภัยไซเบอร์ (Incident Response Plan) ส่วนในระดับบุคคล สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักงานพัฒนารัฐบาลดิจิทัล และสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ควรมีการพัฒนาบุคลากรเพื่อสร้างความตระหนักรู้และจิตสำนึกเกี่ยวกับภัยคุกคามทางไซเบอร์ และการปกป้องคุ้มครองข้อมูลส่วนบุคคลให้กับบุคลากรทุกระดับของหน่วยงานภาครัฐอย่างต่อเนื่อง

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายพรหมินทร์ เลิศสุริย์เดช)
เลขาธิการนายกรัฐมนตรี

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทร. ๐ ๒๒๘๘ ๔๐๐๐ ต่อ ๔๔๐๖
ไปรษณีย์อิเล็กทรอนิกส์ : saraban@thaigov.go.th

สำเนาถูกต้อง
ปัญฑารีย์ ดีประเสริฐไชย
(นางสาวปัญฑารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
- 2 ก.ย. 2568

ด่วนที่สุด
ที่ นร ๐๗๐๘/ว๒๕

สำนักงบประมาณ
๑๐๖๓ ถนนพหลโยธิน
แขวงพญาไท กรุงเทพฯ ๑๐๔๐๐

๒๙ สิงหาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรีขอให้สำนักงบประมาณเสนอความเห็นในส่วนที่เกี่ยวข้องเพื่อประกอบการพิจารณาของคณะรัฐมนตรี กรณีคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอเรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล เพื่อให้คณะรัฐมนตรีพิจารณา ดังนี้

๑. เห็นชอบกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

๒. อนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงานต่อไป

ความละเอียดแจ้งแล้ว นั้น

สำนักงบประมาณพิจารณาแล้วขอเรียนว่า กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล มีวัตถุประสงค์เพื่อขับเคลื่อนการแก้ไขปัญหาเชิงระบบสำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ อาทิ การกำหนดขอบเขตของงานพัฒนาระบบหน่วยงานที่มีมาตรฐาน จัดให้มีการตรวจสอบและประเมินผลการทำงานของระบบอย่างสม่ำเสมอ ตลอดจนจัดอบรมสำหรับผู้พัฒนาและบุคลากรที่เกี่ยวข้องในเรื่องการออกแบบและพัฒนาระบบให้ปลอดภัย ส่งผลให้ระบบดิจิทัลของรัฐมีความมั่นคงปลอดภัย เพิ่มความเชื่อมั่นให้แก่ประชาชน ภาคธุรกิจ และนักลงทุน ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้มีมติเห็นชอบแนวทางดังกล่าว ในคราวประชุมครั้งที่ ๓/๒๕๖๗ เมื่อวันที่ ๓๐ ตุลาคม ๒๕๖๗ แล้ว จึงเห็นสมควรที่คณะรัฐมนตรีจะพิจารณาให้ความเห็นชอบ

/ในหลักการ...

ในหลักการแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล และอนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงาน ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ สำหรับค่าใช้จ่ายที่จะเกิดขึ้น เห็นควรให้หน่วยงานที่เกี่ยวข้องใช้จ่ายจากงบประมาณรายจ่ายประจำปีที่ได้รับจัดสรร หรือพิจารณาปรับแผนการปฏิบัติงานและแผนการใช้จ่ายงบประมาณ โดยโอนงบประมาณรายจ่าย โอนเงินจัดสรรหรือเปลี่ยนแปลงเงินจัดสรร ตามระเบียบว่าด้วยการบริหารงบประมาณ พ.ศ. ๒๕๖๒ และที่แก้ไขเพิ่มเติม แล้วแต่กรณี หรือจัดทำแผนการปฏิบัติงานและแผนการใช้จ่ายงบประมาณ เพื่อเสนอขอตั้งงบประมาณรายจ่ายประจำปีตามความจำเป็นและเหมาะสมตามขั้นตอนต่อไป

จึงเรียนมาเพื่อโปรดนำเสนอความเห็นประกอบการพิจารณาของคณะรัฐมนตรีต่อไป

ขอแสดงความนับถือ

(นายอนันต์ แก้วกำเนิด)
ผู้อำนวยการสำนักงบประมาณ

กองจัดทำงบประมาณด้านเศรษฐกิจ ๓
โทร. ๐ ๒๒๗๘ ๗๐๐๐ ต่อ ๑๒๗๑
ไปรษณีย์อิเล็กทรอนิกส์ saraban@bb.go.th

สำเนาถูกต้อง

ปัญฑารีย์ ดีประเสริฐไชย

(นางสาวปัญฑารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ

- 2 ก.ย. 2568

ด่วนที่สุด
ที่ นร ๐๙๐๗/ ๘๘

สำนักงานคณะกรรมการกฤษฎีกา
๑ ถนนพระอาทิตย์ เขตพระนคร
กรุงเทพฯ ๑๐๒๐๐

๒๐ พฤษภาคม ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามหนังสือที่อ้างถึง สำนักเลขาธิการคณะรัฐมนตรีขอให้สำนักงานคณะกรรมการกฤษฎีกาเสนอความเห็นในส่วนที่เกี่ยวข้องกับเรื่องดังกล่าวตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เสนอ เพื่อประกอบการพิจารณาของคณะรัฐมนตรีโดยด่วน ความละเอียดทราบแล้ว นั้น

สำนักงานคณะกรรมการกฤษฎีกาพิจารณาแล้ว เห็นว่า กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอต่อคณะรัฐมนตรีเพื่อพิจารณาให้ความเห็นชอบและขออนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงานต่อไป เป็นการดำเนินการตามหน้าที่และอำนาจของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการเสนอแนะและให้ความเห็นต่อคณะรัฐมนตรีเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๙ (๑๐) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กรณีจึงเป็นอำนาจของคณะรัฐมนตรีที่จะพิจารณาให้ความเห็นชอบและอนุมัติตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอได้ตามที่เห็นสมควร

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายปกรณ์ นิลประพันธ์)
เลขาธิการคณะกรรมการกฤษฎีกา

กองกฎหมายเทคโนโลยีและการคมนาคม
ฝ่ายกฎหมายเทคโนโลยีและการพลังงาน
โทร. ๐ ๒๒๒๒ ๐๒๐๖ - ๙ ต่อ ๑๑๔๓ (นายธิติฯ)
โทรสาร ๐ ๒๒๒๖ ๖๒๐๑
www.ocs.go.th
www.lawreform.go.th
ไปรษณีย์อิเล็กทรอนิกส์ saracan@ocs.go.th

สำเนาถูกต้อง
ปัญฑารีย์ ดีประเสริฐไชย
(นางสาวปัญฑารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
- 2 มิ.ย. 2568

ที่ นร ๑๑๑๖/๒๘๕๓

สำนักงานสภาพัฒนาการ
เศรษฐกิจและสังคมแห่งชาติ
๙๖๒ ถนนกรุงเกษม กรุงเทพฯ ๑๐๑๐๐

๑๗ มิถุนายน ๒๕๖๘

เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามที่สำนักเลขาธิการคณะรัฐมนตรีขอให้สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติเสนอความเห็นในส่วนที่เกี่ยวข้องเพื่อประกอบการพิจารณาของคณะรัฐมนตรี เรื่อง กรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล ที่เสนอโดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ความละเอียดแจ้งแล้วนั้น

สำนักงานสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติพิจารณาแล้ว มีความเห็นดังนี้

๑. เห็นควรให้ความเห็นชอบกรอบแนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหลและอนุมัติให้ทุกหน่วยงานนำไปดำเนินการเพื่อเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับระบบงานของหน่วยงานต่อไป

๒. สกมช. ควรสร้างความรู้ความเข้าใจในการพิจารณาประยุกต์ใช้มาตรฐาน ISO/IEC ๒๗๐๐๑ หรือ NIST Cyber Security Framework สำหรับหน่วยงานรัฐในการกำหนดขอบเขตของงานพัฒนาระบบโดยเน้นหัวข้อที่มีลำดับความสำคัญก่อนเพื่อให้หน่วยงานรัฐมีระยะเวลาในการเตรียมความพร้อมและจัดหางบประมาณ และหารือกับสำนักงบประมาณในการพิจารณาจัดสรรงบประมาณให้หน่วยงานที่เกี่ยวข้องให้เหมาะสมสำหรับการบริหารจัดการความเสี่ยงในการจัดทำโครงการพัฒนาระบบและการฝึกอบรมพัฒนาบุคลากรด้านเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐได้อย่างเหมาะสมและเกิดประสิทธิภาพ นอกจากนี้ควรมีแนวทางที่ยืดหยุ่นและการสนับสนุนที่เหมาะสมในการกำหนดเกณฑ์ให้บริษัทพัฒนาซอฟท์แวร์มีมาตรฐานที่ผ่านการรับรองทางความปลอดภัย เพื่อให้กลุ่มธุรกิจ Startup และผู้ประกอบการ SMEs เตรียมความพร้อมก่อนมีการบังคับใช้กรอบแนวทางดังกล่าว ซึ่งจะเป็นการสนับสนุนภาคธุรกิจขนาดกลางและ

/ขนาดย่อม...

ขนาดย่อมให้สามารถดำเนินธุรกิจได้อย่างยั่งยืน อีกทั้งหน่วยงานภาครัฐที่ได้รับจำนวนเงินงบประมาณสนับสนุนโครงการพัฒนาระบบที่ไม่สูงมากหรือตั้งอยู่ในหน่วยงานส่วนภูมิภาคสามารถสรรหาผู้รับจ้างในกลุ่มผู้ประกอบวิสาหกิจขนาดกลางและขนาดย่อม (SMEs) ได้

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายดนุชา พิชยนันท์)
เลขาธิการสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทร. ๐ ๒๒๘๐ ๔๐๘๕ ต่อ ๕๔๐๑
E-mail : Archan@nesdc.go.th

สำเนาถูกต้อง

ปัญฑารีย์ ดีประเสริฐไชย

(นางสาวปัญฑารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ

- 2 ก.ย. 2568

ด่วนที่สุด

ที่ สพร ๒๕๖๘/๑๕๙๐

๒๗ พฤษภาคม ๒๕๖๘

เรื่อง ตอบกลับกรอบแนวทางการดำเนินการความปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐ สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ด่วนที่สุด ที่ นร ๐๕๐๖/ว(ล) ๑๒๔๗๔ ลงวันที่ ๒๐ พฤษภาคม ๒๕๖๘

ตามที่อ้างถึง สำนักงานคณะกรรมการรักษาความปลอดภัยไซเบอร์แห่งชาติได้เสนอเรื่อง กรอบแนวทางดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้เกิดการรั่วไหล โดยกองวิเคราะห์เรื่องเสนอคณะรัฐมนตรี มีการสอบถามความเห็นในส่วนรายงานการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๓/๒๕๖๗ วาระที่ ๔.๓ เรื่อง แนวทางการดำเนินการสร้างความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานของรัฐสำหรับป้องกันข้อมูลส่วนบุคคลรั่วไหล สำหรับการป้องกันข้อมูลส่วนบุคคลไม่ให้ข้อมูลรั่วไหล มีรายละเอียดการป้องกัน ๘ รายการ ดังนี้

๑. การกำหนดขอบเขตของงานพัฒนาระบบหน่วยงานควรมีการใช้แนวทาง มาตรฐาน ISO/IEC 27001 หรือ NIST ในการออกแบบ พัฒนา และบำรุงรักษาระบบ งดใช้ข้อมูลจริงในขั้นตอนการพัฒนาระบบ หรือกำหนดให้ใช้ข้อมูลเพื่อทดสอบให้แล้วเสร็จและลบออกภายในระยะเวลา ๓ วัน รวมทั้ง กำหนดเกณฑ์สำหรับการเลือกบริษัทพัฒนาซอฟต์แวร์ที่มีประสบการณ์และมาตรฐานที่ผ่านการรับรองทางความปลอดภัยตลอดจนกำหนดให้มีการทดสอบความปลอดภัยระบบเป็นประจำ ทั้งในช่วงการพัฒนาและก่อนการใช้งานจริงเพื่อค้นหาช่องโหว่และแก้ไขทันที

๒. หน่วยงานควรจัดการอบรมสำหรับผู้พัฒนาและบุคลากรที่เกี่ยวข้องในเรื่อง การออกแบบและพัฒนาระบบให้ปลอดภัย พร้อมสร้างความรับรู้ในเรื่องภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น

๓. จัดให้มีการตรวจสอบและประเมินผลการทำงานของระบบอย่างสม่ำเสมอ รวมถึงการตรวจสอบความสอดคล้องกับมาตรฐานความปลอดภัยที่กำหนด

๔. กำหนดให้มีการระบุเงื่อนไขด้านความปลอดภัยในสัญญาว่าจ้างผู้พัฒนา โดยเน้นความรับผิดชอบต่อปัญหาด้านความปลอดภัยที่อาจเกิดขึ้นจากการพัฒนา

๕. สร้างระบบเฝ้าระวังเพื่อแจ้งเตือนและตอบสนองต่อการโจมตีหรือช่องโหว่ที่ เกิดขึ้นอย่างรวดเร็ว รวมถึงการมีแผนรับมือเมื่อเกิดเหตุการณ์ความปลอดภัยไซเบอร์

๖. สนับสนุนการปรับปรุงระบบให้ทันสมัยอยู่เสมอ โดยอัปเดตซอฟต์แวร์ และแพตช์ด้านความปลอดภัยเมื่อมีช่องโหว่ถูกค้นพบ

๗. หากมีระบบงานที่ไม่ได้ใช้งาน ควรมีการปิดระบบเพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลได้

๘. ให้หน่วยงานยึดหลักตาม Cloud Security Standards และสอดคล้องกับนโยบาย Cloud First Policy เพื่อเสริมสร้างความมั่นคงปลอดภัยทางดิจิทัล

ในการนี้ สำนักงาน...

ในการนี้ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) มีความเห็นในข้อ ๑ ดังนี้

๑. "การกำหนดขอบเขตของงานพัฒนาระบบหน่วยงานควรมีการใช้แนวทาง มาตรฐาน ISO/IEC 27001 หรือ NIST ในการออกแบบ พัฒนา และบำรุงรักษาระบบ" สำนักงานเห็นว่าควรให้ความชัดเจนในประเด็นนี้ ในส่วนของงานที่มีการจ้างพัฒนาจากภายนอกหรือหน่วยงานรัฐจำเป็นต้องผ่านการรับรองมาตรฐาน ISO/IEC 27001 ในงานที่เกี่ยวข้องในการพัฒนาออกแบบหรือไม่ เพราะจะมีผลต่อการขอใบรับรอง และเกิดค่าใช้จ่ายของหน่วยงานรัฐ หรือหน่วยงานภายนอกที่ต้องดำเนินการ

๒. "กำหนดให้ใช้ข้อมูลเพื่อทดสอบให้แล้วเสร็จและลบออกภายในระยะเวลา ๓ วัน" สำนักงานเห็นว่า ควรมีการระบุความชัดเจนของข้อความที่ครอบคลุมถึงวิธีการลบ หรือทำลายที่ปลอดภัย พร้อมระบุให้ทวนสอบการลบข้อมูลหรือทำลาย ว่าข้อมูลไม่สามารถนำกลับมาใช้งานได้

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการ รักษาการแทน
ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

ฝ่ายความมั่นคงปลอดภัยไซเบอร์
ส่วนแผนงานและที่ปรึกษาความมั่นคงปลอดภัยไซเบอร์
มือถือ ๐๘ ๐๐๔๕ ๓๑๖๓ (ศรีสุดา)
ไปรษณีย์อิเล็กทรอนิกส์ cbp_division@dga.or.th
ไปรษณีย์อิเล็กทรอนิกส์สารบรรณกลาง saraban@dga.or.th

สำเนาถูกต้อง
ปัญฑารีย์ ดีประเสริฐไชย
(นางสาวปัญฑารีย์ ดีประเสริฐไชย)
นักวิเคราะห์นโยบายและแผนปฏิบัติการ
- 2 ก.ย. 2568