คำสั่งกรมการขนส่งทางราง
ที่ ๒๙ / ๒๕๖๗
เรื่อง แต่งตั้งผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง
(Chief Information Security Officer : CISO)
ประจำกรมการขนส่งทางราง

ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ – ๒๕๗๐) ข้อ ๑ การกำกับดูแล การรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity) ข้อ ๑.๓ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่า ที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน ประกอบกับกรมการขนส่งทางรางมีการบริการที่ให้ประชาชนได้เข้าถึงและใช้บริการโดยมีวัตถุประสงค์เพื่ออำนวยความสะดวกให้ประชาชน นั้น

เพื่อให้กรมการขนส่งทางรางสามารถรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบหรือก่อให้เกิดความเสี่ยงต่อการให้บริการซึ่งจะเป็นอุปสรรคต่อการบรรลุเป้าประสงค์ จึงให้ดำเนินการดังต่อไปนี้

๑. ให้รองอธิบดีกรมการขนส่งทางราง เป็นผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) ประจำกรมการขนส่งทางราง

๒. บทบาทหน้าที่

๒.๑ กำหนดนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งกำกับดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด

๒.๒ กำหนดคุณลักษณะด้านความมั่นคงปลอดภัย (Security Specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT Security Architecture)

๒.๓ บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงที่องค์กรมี และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการหน่วยงานเป็นวาระประจำ

๒.๔ ดูแลและดำเนินการให้หน่วยงานมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

๒.๕ ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้ เรื่องความเสี่ยงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านภัยคุกคามทางไซเบอร์

/๒.๖ รายงานปัญหา...

๒.๖ รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด คณะกรรมการของหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และคณะกรรมการที่เกี่ยวข้องโดยตรง

๒.๗ ให้ความเห็นด้านภัยคุกคามไซเบอร์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการศูนย์รักษาความมั่นคงปลอดภัยไซเบอร์ของระบบขนส่งทางรางและคณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศและร่วมตัดสินใจในการดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ที่กระทบต่อกรมการขนส่งทางราง และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒.๘ อนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของกรมการขนส่งทางราง และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จากภัยคุกคามทางไซเบอร์

๒.๙ ต้องทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติกับสภาพแวดล้อมการปฏิบัติการไซเบอร์ของบริการที่สำคัญของกรมการขนส่งทางราง และภูมิทัศน์ภัยคุกคามทางไซเบอร์ในปัจจุบันอย่างน้อยปีละหนึ่งครั้งนับถัดจากวันที่การทบทวนครั้งสุดท้ายหรือวันที่มีผลบังคับใช้นโยบาย มาตรฐาน หรือแนวปฏิบัติ

๒.๑๐ ปฏิบัติภารกิจอื่นที่เกี่ยวข้องกับความมั่นคงและปลอดภัยสารสนเทศระดับสูงตามที่ได้รับมอบหมาย

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๗ กุมภาพันธ์ พ.ศ. ๒๕๖๗

(นายพิเชฐ คุณาธรรมรักษ์)
อธิบดีกรมการขนส่งทางราง