บันทึกท้ายพระราชบัญญัติ
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ความเป็นมา

พระราชบัญญัติพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีเจตนารมณ์เพื่อจัดให้มีกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อป้องกันความเสียงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ โดยคณะรัฐมนตรีได้เสนอต่อประธานสภานิติบัญญัติแห่งชาติ เมื่อวันที่ เมื่อวันที่ ๒๖ ธันวาคม ๒๕๖๑ เพื่อให้พิจารณาตามบทบัญญัติรัฐธรรมนูญแห่งราชอาณาจักรไทย ซึ่งประธานสภานิติบัญญัติแห่งชาติบรรจุในระเบียบวาระการประชุมสภานิติบัญญัติแห่งชาติ ครั้งที่ ๙๑/๒๕๖๑ วันศุกร์ที่ ๒๘ ธันวาคม ๒๕๖๑ และในคราวประชุมสภานิติบัญญัติแห่งชาติ ครั้งที่ ๑๙/๒๕๖๒ เป็นพิเศษ ในวันพฤหัสบดีที่ ๒๘ กุมภาพันธ์ ๒๕๖๒ ที่ประชุมได้พิจารณาในวาระที่ ๒ และลงมติในวาระที่ ๓ เห็นสมควรประกาศใช้เป็นกฎหมาย โดยส่งร่างพระราชบัญญัติดังกล่าวไปยังนายกรัฐมนตรีเพื่อนำขึ้นทูลเกล้าฯ วันที่ ๑๑ มีนาคม ๒๕๖๒

ประกาศในราชกิจจานุเบกษา เล่ม ๑๓๖ ตอน ๖๙ ก วันที่ ๒๗ พฤษภาคม ๒๕๖๒ หน้า ๒๐

วันเริ่มใช้บังคับ ตั้งแต่วันที่ ๒๘ พฤษภาคม ๒๕๖๒ เป็นต้นไป

ผู้รักษาการ นายกรัฐมนตรี

เหตุผลในการประกาศใช้

โดยที่ในปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้น เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที สมควรกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและหน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพและต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นต้องตราพระราชบัญญัตินี้

สาระสำคัญของพระราชบัญญัติ

พระราชบัญญัติพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มีบทบัญญัติทั้งสิ้น ๘๓ มาตรา สาระสำคัญสรุปได้ดังนี้

๑. กำหนดนิยามความหมายของคำว่า “การรักษาความมั่นคงปลอดภัยไซเบอร์” “ภัยคุกคามทางไซเบอร์” “ไซเบอร์” “หน่วยงานของรัฐ” “ประมวลแนวทางปฏิบัติ” “เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” “มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์” “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” “หน่วยงานควบคุมหรือกำกับดูแล” “คณะกรรมการ” “พนักงานเจ้าหน้าที่” “เลขาธิการ” “สำนักงาน” “รัฐมนตรี” (มาตรา ๓)

๒. กำหนดให้นายกรัฐมนตรีรักษาการตามพระราชบัญญัตินี้ (มาตรา ๔)

๓. กำหนดให้มีคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรียกโดยย่อว่า “กมช.” และให้ใช้ชื่อเป็นภาษาอังกฤษว่า “National Cyber Security Committee” โดยเรียกย่อว่า “NCSC” (มาตรา ๕)

๔. กำหนดให้คณะกรรมการมีหน้าที่และอำนาจในการเสนอนโยบายและแผน กำหนดนโยบายการบริหารจัดการ จัดทำแผนปฏิบัติการ กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการ กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ ประสานความร่วมมือกับหน่วยงานอื่น ตามที่กำหนดไว้ในมาตรา ๙ แห่งพระราชบัญญัตินี้ (มาตรา ๙)

๕. กำหนดให้มีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กกม.” ในการกำกับดูแลการดำเนินการตามหน้าที่และอำนาจของคณะกรรมการ

๖. กำหนดให้ กกม. มีหน้าที่และอำนาจ ตามที่กำหนดไว้ในมาตรา ๑๓ แห่งพระราชบัญญัตินี้ (มาตรา ๑๓)

๗. กำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น (มาตรา ๒๐)

๘. กำหนดให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรับผิดชอบงานธุรการ งานวิชาการ งานการประชุมและงานเลขานุการของคณะกรรมการ และ กกม. และให้มีหน้าที่และอำนาจตามที่กำหนดไว้ในมาตรา ๒๒ และมีหน้าที่และอำนาจทั่วไปตามที่กำหนดไว้ในมาตรา ๒๓ แห่งพระราชบัญญัตินี้ (มาตรา ๒๒, มาตรา ๒๓)

๙. กำหนดให้มีคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กบส.” เพื่อดูแลงานด้านกิจการบริหารงานทั่วไปของสำนักงาน (มาตรา ๒๕)

๑๐. กำหนดให้ กบส. มีหน้าที่และอำนาจตามที่กำหนดไว้ในมาตรา ๒๗ แห่งพระราชบัญญัตินี้ (มาตรา ๒๗)

๑๑. กำหนดให้การรักษาความมั่นคงปลอดภัยไซเบอร์ต้องคำนึงถึงความเป็นเอกภาพและบูรณาการในการดำเนินงานของหน่วยงานของรัฐและหน่วยงานเอกชน และต้องสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ การดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมุ่งหมายเพื่อสร้างศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (มาตรา ๔๑)

๑๒. กำหนดนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีเป้าหมายและแนวทางอย่างน้อยตามที่กำหนดไว้ในมาตรา ๔๒ แห่งพระราชบัญญัตินี้ (มาตรา ๔๒)

๑๓. กำหนดให้คณะกรรมการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นตามแนวทางในมาตรา ๔๒ เพื่อเสนอคณะรัฐมนตรีให้ความเห็นชอบ โดยให้ประกาศในราชกิจจานุเบกษา และเมื่อได้ประกาศแล้วให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามทีกำหนดไว้ในแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการให้เป็นไปตามนโยบายและแผนดังกล่าว (มาตรา ๔๓)

๑๔. กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องประกอบไปด้วยรายละเอียดตามที่กำหนดไว้ในมาตรา ๔๔ แห่งพระราชบัญญัตินี้ (มาตรา ๔๔)

๑๕. กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) (มาตรา ๔๕)

๑๖. กำหนดให้สำนักงานให้การสนับสนุนและให้ความช่วยเหลือในการป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีความมั่นคงของรัฐ ความมั่นคงทางทหาร ความมั่นคงทางเศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ (มาตรา ๔๘)

๑๗. กำหนดให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค ด้านสาธารณสุข และด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (มาตรา ๔๙)

๑๘. กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมินทั้งโดยผู้ตรวจภายในและผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละหนึ่งครั้ง (มาตรา ๕๔)

๑๙. กำหนดให้ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นตรวจสอบข้อมูลที่เกี่ยวข้องเพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ และให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการป้องกันความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น (มาตรา ๕๘)

๒๐. กำหนดให้การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ คณะกรรมการจะกำหนดลักษณะของภัยคุกคามทางไซเบอร์โดยแบ่งออกเป็นสามระดับ ได้แก่ (๑) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง (๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง (๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติตามที่กำหนดรายละเอียดไว้ในมาตรา ๖๐ แห่งพระราชบัญญัตินี้ (มาตรา ๖๐)

๒๑. กำหนดให้เมื่อเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ กกม. ออกคำสั่งให้สำนักงานดำเนินการรวบรวมข้อมูล สนับสนุนให้ความช่วยเหลือในการป้องกัน รับมือในด้านต่าง ๆ ตามที่กำหนดไว้ในมาตรา ๖๑ แห่งพระราชบัญญัตินี้ (มาตรา ๖๑)

๒๒. กำหนดให้ในกรณีที่มีความจำเป็นเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้ กกม. มีคำสั่งให้หน่วยงานของรัฐให้ข้อมูล สนับสนุนบุคลากรในสังกัดหรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่มีอยู่ในความครอบครองเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (มาตรา ๖๓)

๒๓. กำหนดให้ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ให้ กกม. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ โดยการดำเนินการตามที่ระบุไว้ในมาตรา ๖๕ แห่งพระราชบัญญัตินี้ (มาตรา ๖๕)

๒๔. กำหนดให้ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ในการเข้าตรวจสอบสถานที่ การเข้าถึงข้อมูลคอมพิวเตอร์ การทำสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ การยัดหรืออายัดคอมพิวเตอร์ ตามที่ระบุไว้ในมาตรา ๖๖ แห่งพระราชบัญญัตินี้ (มาตรา ๖๖)

๒๕. กำหนดให้ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติในกาดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง (มาตรา ๖๗)

๒๖. กำหนดให้ในกรณีที่เป็นเหตุจำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ คณะกรรมการอาจมอบหมายให้เลขาธิการมีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้โดยไม่ต้องยื่นคำร้องต่อศาล (มาตรา ๖๘)

๒๗. ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ (มาตรา ๗๐)

๒๘. กำหนดให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้หากผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามพระราชบัญญัตินี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ (มาตรา ๗๑)

๒๙. ผู้ใดล่วงรู้ข้อมูลตามพระราชบัญญัตินี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ (มาตรา ๗๒)

๓๐. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่รายงานเหตุภัยคุกคามทางไซเบอร์ตามมาตรา ๕๗ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท (มาตรา ๗๓)

๓๑. ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กกม. ตามมาตรา ๖๕ (๑) และ (๒) โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสามแสนบาท และปรับอีกไม่เกินวันละหนึ่งหมื่นบาทนับแต่วันที่ครบกำหนดระยะเวลาที่ กกม. ออกคำสั่งให้ปฏิบัติจนกว่าจะปฏิบัติให้ถูกต้อง และผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งตามมาตรา ๖๕ (๓) และ (๔) หรือไม่ปฏิบัติตามคำสั่งศาลตามมาตรา ๖๕ (๕) ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ (มาตรา ๗๕)

๓๒. ผู้ใดขัดขวาง หรือไม่ปฏิบัติตามคำสั่งของ กกม. หรือพนักงานเจ้าหน้าที่ซึ่งปฏิบัติตามคำสั่งของ กกม. ตามมาตรา ๖๖ (๑) หรือไม่ปฏิบัติตามคำสั่งศาลตามมาตรา ๖๖ (๒) (๓) หรือ (๔) โดยไม่มีเหตุอันสมควร ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ (มาตรา ๗๖)

๓๓. กำหนดให้ในกรณีที่ผู้กระทำผิดตามพระราชบัญญัตินี้เป็นนิติบุคคลถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการหรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้น

ไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย (มาตรา ๗๗)

นางสาวจุฬาพัฒน์ ช่างเกตุ / จัดทำ