บันทึกหลักการและเหตุผล
ประกอบร่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (ฉบับที่ ..)
พ.ศ. ....

หลักการ

แก้ไขเพิ่มเติมพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ดังต่อไปนี้

(๑) ปรับปรุงบทนิยามโดยแก้ไขเพิ่มเติมบทนิยามคำว่า “การรักษาความมั่นคงปลอดภัยไซเบอร์” “ภัยคุกคามทางไซเบอร์” “ไซเบอร์ “โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” และ “สำนักงาน” เพิ่มบทนิยามคำว่า “รับมือ” “เหตุภัยคุกคามทางไซเบอร์ “ระบบคอมพิวเตอร์” “ข้อมูลคอมพิวเตอร์” “หน่วยงานภารกิจพิเศษ” “กกม.” และ “กบส.” และยกเลิกบทนิยามคำว่า “ประมวลแนวทางปฏิบัติ” “เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” และ “มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์” และบทบัญญัติที่เกี่ยวข้องกับการปรับปรุงบทนิยามดังกล่าว (แก้ไขเพิ่มเติมมาตรา ๓ มาตรา ๑๔ วรรคหนึ่ง มาตรา ๒๒ และมาตรา ๒๓ (๕))

(๒) กำหนดคุณสมบัติของกรรมการผู้ทรงคุณวุฒิในคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในเรื่องการไม่มีผลประโยชน์ทับซ้อนกับการปฏิบัติหน้าที่ (เพิ่มมาตรา ๖ (๗) และมาตรา ๓๑ (๙))

(๓) แก้ไขเพิ่มเติมบทบัญญัติที่เกี่ยวกับหน้าที่และอำนาจของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ และหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการรักษาความมั่นคงปลอดภัยไซเบอร์และในการจัดการความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมทั้งการรับมือเหตุภัยคุกคามทางไซเบอร์ให้ชัดเจนยิ่งขึ้นและสอดคล้องกับการดำเนินการตามหลักสากล รวมถึงแก้ไขเพิ่มเติมบทกำหนดโทษที่เกี่ยวข้อง (แก้ไขเพิ่มเติมมาตรา ๙ มาตรา ๑๓ มาตรา ๔๑ มาตรา ๔๒ (๒) มาตรา ๔๓ มาตรา ๔๔ มาตรา ๔๕ วรรคหนึ่ง มาตรา ๕๐ วรรคหนึ่ง มาตรา ๕๓ วรรคสอง มาตรา ๕๖ มาตรา ๕๗ มาตรา ๕๘ มาตรา ๖๐ มาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ วรรคหนึ่ง มาตรา ๖๔ มาตรา ๖๕ วรรคหนึ่ง มาตรา ๖๖ มาตรา ๖๗ มาตรา ๖๘ มาตรา ๖๙ และมาตรา ๗๓ และเพิ่มมาตรา ๔๒ (๙) มาตรา ๕๘/๑ มาตรา ๕๘/๒ มาตรา ๕๘/๓ มาตรา ๖๐/๑ มาตรา ๗๒/๑ มาตรา ๗๔ วรรคสอง มาตรา ๗๔/๑ และมาตรา ๗๖/๑)

(๔) แก้ไขเพิ่มเติมองค์ประกอบของคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ในส่วนกรรมการผู้ทรงคุณวุฒิ (แก้ไขเพิ่มเติมมาตรา ๑๒ (๓))

(๕) แก้ไขเพิ่มเติมชื่อสำนักงานและคณะกรรมการบริหารสำนักงาน และกำหนดหน้าที่และอำนาจของคณะกรรมการบริหารสำนักงานในการกำหนดเครื่องแบบ เครื่องหมายหรือสัญลักษณ์ (แก้ไขเพิ่มเติมชื่อหมวด ๒ มาตรา ๒๐ และมาตรา ๒๕ วรรคหนึ่ง และเพิ่มมาตรา ๒๗ (๖/๑))

(๖) กำหนดให้เงินและทรัพย์สินของสำนักงานไม่ต้องนำส่งคลังเป็นรายได้แผ่นดิน (แก้ไขเพิ่มเติมมาตรา ๒๔ วรรคสอง)

(๗) แก้ไขเพิ่มเติมด้านของภารกิจหรือให้บริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (แก้ไขเพิ่มเติมมาตรา ๔๘ และเพิ่มมาตรา ๔๙ (๗/๑))

(๘) กำหนดให้คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์มีอำนาจและหน้าที่ในการกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการป้องกัน รับมือ หรือลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ของหน่วยงานภารกิจพิเศษที่ได้รับมอบหมายจากคณะรัฐมนตรีหรือคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้ปฏิบัติภารกิจเป็นการชั่วคราว (เพิ่มมาตรา ๔๙/๑)

(๙) กำหนดให้สำนักงานมีอำนาจในการตรวจสอบหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีหน้าที่กำกับและติดตามผู้ให้บริการภายนอกของตนให้ดำเนินการตามมาตรฐานที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติหรือคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด หรือตามที่พระราชบัญญัตินี้กำหนด (เพิ่มมาตรา ๕๔/๑ มาตรา ๕๔/๒ และมาตรา ๕๔/๓)

(๑๐) กำหนดให้การใช้หรือเปิดเผยข้อมูลที่ได้รับจากการรายงานเหตุภัยคุกคามทางไซเบอร์ได้เฉพาะกรณีให้การช่วยเหลือหน่วยงานเจ้าของระบบสารสนเทศ รวมถึงบุคคลหรือหน่วยงานที่ได้รับมอบหมายหรือที่ปฏิบัติการแทนหน่วยงานเจ้าของระบบสารสนเทศที่ได้รับผลกระทบ หรือกรณีอื่นที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด (เพิ่มมาตรา ๕๙/๑)

(๑๑) กำหนดให้พนักงานเจ้าหน้าที่มีอำนาจในการสืบสวนสอบสวนความผิดตามพระราชบัญญัตินี้ (เพิ่มมาตรา ๖๙/๑)

(๑๒) กำหนดให้ความผิดตามพระราชบัญญัตินี้เป็นความผิดที่สามารถเปรียบเทียบปรับได้ (เพิ่มมาตรา ๗๗/๑)

เหตุผล

โดยที่ระบบเทคโนโลยีสารสนเทศเป็นปัจจัยประการหนึ่งที่สำคัญต่อการพัฒนาประเทศทั้งทางด้านเศรษฐกิจและสังคม รวมทั้งมีผลต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ประกอบกับระบบเทคโนโลยีสารสนเทศมีความก้าวหน้าอย่างรวดเร็ว ทำให้ความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กระทบต่อความมั่นคงปลอดภัยของประเทศ ความสัมพันธ์ระหว่างประเทศ ความมั่นคงทางเศรษฐกิจและความปลอดภัยสาธารณะหรือความสงบเรียบร้อยภายในประเทศ มีโอกาสเกิดได้มากขึ้น สมควรปรับปรุงหน้าที่และอำนาจขององค์กรหรือหน่วยงานทั้งภาครัฐและภาคเอกชนที่เกี่ยวข้อง รวมถึงพนักงานเจ้าหน้าที่ที่ต้องปฏิบัติการในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สามารถกำหนดมาตรการที่เหมาะสมในการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงมาตรการรับมือเหตุภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที ตลอดจนปรับปรุงหลักเกณฑ์และแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ชัดเจนและเหมาะสมยิ่งขึ้น อันจะทำให้การป้องกันภัยคุกคามทางไซเบอร์และการรับมือเหตุภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นต้องตราพระราชบัญญัตินี้

ร่าง
พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์ (ฉบับที่ ..)
พ.ศ. ....

.....
.....
.....

.....
.....

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

.....
.....

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (ฉบับที่ ..) พ.ศ. ....”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้ยกเลิกมาตรา ๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๓ ในพระราชบัญญัตินี้

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ซึ่งกระทบต่อความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความปลอดภัยสาธารณะหรือความสงบเรียบร้อยภายในประเทศ

“รับมือ” หมายความว่า เตรียมการ ตรวจจับ วิเคราะห์ ระงับ และกำจัด ภัยคุกคามทางไซเบอร์หรือเหตุภัยคุกคามทางไซเบอร์ และให้หมายความรวมถึงดำเนินการใดที่เกี่ยวข้องเพื่อแก้ไข บรรเทาหรือฟื้นฟูความเสียหายภายหลังเกิดเหตุภัยคุกคามทางไซเบอร์ดังกล่าว ตลอดจนนำเหตุภัยคุกคามทางไซเบอร์นั้นมาศึกษาเพื่อหาแนวทางป้องกันมิให้เกิดซ้ำอีก

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบด้วยกฎหมาย โดยใช้คอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ ไม่ว่าจากภายในประเทศหรือภายนอกประเทศ ที่อาจก่อความเสียหายหรือผลกระทบต่อการดำเนินการ ภาพลักษณ์ ชื่อเสียง ทรัพย์สิน หรือบุคลากร ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือหน่วยงานเอกชน

“เหตุภัยคุกคามทางไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือหน่วยงานเอกชน และทำให้เกิดหรือคาดว่าจะเกิดความเสียหายหรือผลกระทบต่อความสามารถในการรักษาความลับ ความถูกต้องครบถ้วน หรือสภาพพร้อมใช้งานของคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง ของหน่วยงานดังกล่าว

“ไซเบอร์” หมายความว่า ระบบเครือข่ายข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เทคโนโลยีสารสนเทศ เครือข่ายคอมพิวเตอร์ เครือข่ายอินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือระบบสื่อสารอื่นใดที่มีการเชื่อมต่อกันอย่างเป็นระบบ รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ ความมั่นคงทางเศรษฐกิจของประเทศ ความปลอดภัยสาธารณะหรือความสงบเรียบร้อยภายในประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“หน่วยงานควบคุมหรือกำกับดูแล” หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

“หน่วยงานภารกิจพิเศษ” หมายความว่า คณะบุคคลหรือนิติบุคคลที่ได้รับมอบหมายจากคณะรัฐมนตรีหรือคณะกรรมการให้ดำเนินการอย่างหนึ่งอย่างใดเป็นการชั่วคราวหรือภายในระยะเวลาที่กำหนด

“คณะกรรมการ” หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“กกม.” หมายความว่า คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

“กบส.” หมายความว่า คณะกรรมการบริหารสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“เลขาธิการ” หมายความว่า เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“สำนักงาน” หมายความว่า สำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้”

มาตรา ๔ ให้เพิ่มความต่อไปนี้เป็น (๗) ของมาตรา ๖ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“(๗) เป็นบุคคลซึ่งมีผลประโยชน์ทับซ้อนหรือขัดกับการปฏิบัติหน้าที่กรรมการ หรือเป็นบุคคลที่ปฏิบัติหน้าที่หรือประกอบการในกิจการของหน่วยงานของรัฐหรือหน่วยงานเอกชนซึ่งมีผลประโยชน์ทับซ้อนหรือขัดกับการปฏิบัติหน้าที่กรรมการ”

มาตรา ๕ ให้ยกเลิกความในมาตรา ๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๙ คณะกรรมการมีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมและสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๒ และมาตรา ๔๓ ต่อคณะรัฐมนตรีเพื่อให้ความเห็นชอบ ซึ่งต้องเป็นไปตามแนวทางที่กำหนดไว้ในมาตรา ๔๒

(๒) เสนอแนะและให้ความเห็นต่อคณะรัฐมนตรีให้มีการกำหนดมาตรการหรือแรงจูงใจทางการเงินการคลังหรือประโยชน์อื่น เพื่อส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์

(๓) จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรีสำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติ รวมถึงการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และในสถานการณ์ที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์และเหตุภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบายและแผนตาม (๑) รวมถึงนโยบายยุทธศาสตร์ชาติ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ และแผนระดับชาติในเรื่องที่เกี่ยวข้อง ตลอดจนนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

(๔) กำหนดมาตรฐานการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานเอกชน และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์หรือระบบคอมพิวเตอร์ รวมถึงกำหนดมาตรฐานการให้บริการหรือผลิตภัณฑ์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนกำหนดมาตรการหรือแนวทางในการรับรองหน่วยงานที่ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามมาตรฐานที่กำหนด

(๕) กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๖) กำหนดกรอบการประสานความร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๗) แต่งตั้งและถอดถอนเลขาธิการ

(๘) มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนด วัตถุประสงค์ หน้าที่และอำนาจ และกรอบการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๙) ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่บัญญัติไว้ในพระราชบัญญัตินี้

(๑๐) เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติหรือคณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๑) เสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๒) จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ

(๑๓) ปฏิบัติการอื่นใดตามที่บัญญัติไว้ในพระราชบัญญัตินี้ หรือคณะรัฐมนตรีมอบหมาย”

มาตรา ๖ ให้ยกเลิกความใน (๓) ของวรรคหนึ่งของมาตรา ๑๒ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“(๓) กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินสี่คน ซึ่งคณะกรรมการแต่งตั้งจากผู้มีความรู้ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านวิทยาศาสตร์ ด้านวิศวกรรมศาสตร์ ด้านกฎหมาย ด้านการเงิน หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์”

มาตรา ๗ ให้ยกเลิกความในมาตรา ๑๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๑๓ กกม. มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) ติดตามการดำเนินการตามนโยบายและแผนตามมาตรา ๙ (๑) และมาตรา ๔๒

(๒) ดูแลและดำเนินการเพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ตามพระราชบัญญัตินี้ เว้นแต่เป็นกรณีตามมาตรา ๖๗ และมาตรา ๖๘

(๓) กำกับดูแลการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่สอดคล้องกับมาตรฐานการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดในมาตรา ๙ (๔) รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ และมาตรการตอบสนองและรับมือกับเหตุภัยคุกคามทางไซเบอร์ เมื่อมีเหตุภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

(๕) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแลต้องกำหนด

มาตรฐานที่เหมาะสมเพื่อรับมือกับเหตุภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ

(๖) พิจารณา วิเคราะห์สถานการณ์ และประเมินผลกระทบที่เกิดหรือคาดว่าจะเกิดจากเหตุภัยคุกคามทางไซเบอร์เพื่อกำหนดระดับผลกระทบของเหตุภัยคุกคามทางไซเบอร์ พร้อมทั้งการดำเนินการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ในแต่ละระดับ

(๗) พิจารณากำหนดมาตรการตอบโต้เท่าที่จำเป็นโดยคำนึงถึงหลักความได้สัดส่วน เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ ภายใต้หลักกฎหมายระหว่างประเทศในมิติไซเบอร์

(๘) กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ในการกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานตามวรรคหนึ่ง (๔) ให้คำนึงถึงหลักการบริหารความเสี่ยง โดยอย่างน้อยต้องประกอบด้วยมาตรการ ดังต่อไปนี้

(๑) การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ตามหลักการควบคุม กำกับ และตรวจสอบ

(๒) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๓) การป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๔) การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

(๕) การตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์ที่ตรวจพบ

(๖) การฟื้นฟูความเสียหายที่เกิดจากเหตุภัยคุกคามทางไซเบอร์”

มาตรา ๘ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๑๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๑๔ ในการดำเนินการตามมาตรา ๑๓ วรรคหนึ่ง (๒) เพื่อรับมือกับเหตุภัยคุกคามทางไซเบอร์ได้ทันท่วงที กกม. อาจมอบอำนาจให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ผู้บัญชาการทหารสูงสุด และกรรมการอื่นซึ่ง กกม. กำหนด ร่วมกันปฏิบัติการในเรื่องดังกล่าวได้ และจะกำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุนด้วยก็ได้”

มาตรา ๙ ให้ยกเลิกชื่อหมวด ๒ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“หมวด ๒

สำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ”

มาตรา ๑๐ ให้ยกเลิกความในมาตรา ๒๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๒๐ ให้มีสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรียกโดยย่อว่า “สำนักงานไซเบอร์แห่งชาติ” เป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น”

มาตรา ๑๑ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๒๒ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๒๒ ให้สำนักงานรับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของคณะกรรมการ กกม. และ กบส. และให้มีหน้าที่และอำนาจดังต่อไปนี้ด้วย

(๑) เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๙ ต่อคณะกรรมการ

(๒) เสนอประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อ กกม. เพื่อพิจารณากำหนดตามมาตรา ๑๓ วรรคหนึ่ง (๔)

(๓) ประสานงานการดำเนินการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๕๓ และมาตรา ๕๔

(๔) ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในประเทศและต่างประเทศและกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

(๕) ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับเหตุภัยคุกคามทางไซเบอร์

(๖) เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลและการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์หรือเหตุภัยคุกคามทางไซเบอร์

(๗) ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงมาตรการรับมือกับเหตุภัยคุกคามทางไซเบอร์ หรือตามคำสั่งของคณะกรรมการ

(๘) ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ โดยเฉพาะที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๙) เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์หรือเหตุภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน

(๑๐) เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน

(๑๑) เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชนทั้งในประเทศและต่างประเทศ

(๑๒) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน

(๑๓) ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ

(๑๔) ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๕) รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้งปัญหาและอุปสรรค เสนอต่อคณะกรรมการเพื่อพิจารณาดำเนินการ ทั้งนี้ ตามระยะเวลาที่คณะกรรมการกำหนด

(๑๖) ปฏิบัติงานอื่นใดอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามที่คณะรัฐมนตรี คณะกรรมการ หรือ กกม. มอบหมาย”

มาตรา ๑๒ ให้ยกเลิกความใน (๕) ของมาตรา ๒๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“(๕) ปฏิบัติการอื่นใดที่กฎหมายกำหนดให้เป็นหน้าที่และอำนาจของสำนักงาน หรือตามที่คณะกรรมการ กกม. หรือ กบส. มอบหมาย”

มาตรา ๑๓ ให้ยกเลิกความในวรรคสองของมาตรา ๒๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“เงินและทรัพย์สินของสำนักงานตามวรรคหนึ่ง ไม่ต้องนำส่งคลังเป็นรายได้แผ่นดิน”

มาตรา ๑๔ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๒๕ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๒๕ ให้มีคณะกรรมการบริหารสำนักงานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรียกโดยย่อว่า “กบส.” เพื่อดูแลงานด้านกิจการบริหารงานทั่วไปของสำนักงาน ประกอบด้วย รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม อธิบดีกรมบัญชีกลาง เลขาธิการ ก.พ. เลขาธิการ ก.พ.ร. และกรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินหกคน เป็นกรรมการ”

มาตรา ๑๕ ให้เพิ่มความต่อไปนี้เป็น (๖/๑) ของมาตรา ๒๗ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“(๖/๑) กำหนดเครื่องแบบ เครื่องหมายหรือสัญลักษณ์ ของสำนักงาน เลขาธิการ พนักงาน และลูกจ้างของสำนักงาน”

มาตรา ๑๖ ให้เพิ่มความต่อไปนี้เป็น (๙) ของมาตรา ๓๑ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“(๙) เป็นบุคคลซึ่งมีผลประโยชน์ทับซ้อนหรือขัดกับการปฏิบัติหน้าที่เลขาธิการ หรือเป็นบุคคลที่ปฏิบัติหน้าที่หรือประกอบการในกิจการของหน่วยงานของรัฐหรือหน่วยงานเอกชนซึ่งมีผลประโยชน์ทับซ้อนหรือขัดกับการปฏิบัติหน้าที่เลขาธิการ”

มาตรา ๑๗ ให้ยกเลิกความในมาตรา ๔๑ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๔๑ การรักษาความมั่นคงปลอดภัยไซเบอร์ต้องคำนึงถึงความเป็นเอกภาพและการบูรณาการในการดำเนินงานของหน่วยงานของรัฐและหน่วยงานเอกชน และต้องสอดคล้องกับนโยบายยุทธศาสตร์ชาติ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ แผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และแผนระดับชาติในเรื่องที่เกี่ยวข้อง รวมถึงนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

การดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมุ่งหมายเพื่อสร้างศักยภาพและเพิ่มประสิทธิภาพในการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ”

มาตรา ๑๘ ให้ยกเลิกความใน (๒) ของมาตรา ๔๒ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“(๒) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์”

มาตรา ๑๙ ให้เพิ่มความต่อไปนี้เป็น (๙) ของมาตรา ๔๒ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“(๙) การสร้างมาตรการหรือกลไกในการติดตามและประเมินผลการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์”

มาตรา ๒๐ ให้ยกเลิกความในมาตรา ๔๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๔๓ ให้คณะกรรมการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นตามแนวทางในมาตรา ๔๒ รวมทั้งจัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรีเพื่อพิจารณาให้ความเห็นชอบ และให้ประกาศในราชกิจจานุเบกษา

เมื่อได้ประกาศนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์แล้ว ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานที่เกี่ยวข้อง ดำเนินการให้เป็นไปตามนโยบายและแผน รวมถึงแผนปฏิบัติการดังกล่าว

ในการจัดทำนโยบายและแผนตามวรรคหนึ่ง ให้สำนักงานจัดให้มีการรับฟังความเห็นหรือประชุมร่วมกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ”

มาตรา ๒๑ ให้ยกเลิกความในมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำนโยบาย มาตรฐาน และแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์และประมวลแนวทางปฏิบัติและกรอบมาตรฐานตามมาตรา ๑๓ วรรคหนึ่ง (๔) โดยเร็ว

นโยบาย มาตรฐาน และแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่งอย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือเหตุภัยคุกคามทางไซเบอร์

เพื่อประโยชน์ในการจัดทำนโยบาย มาตรฐาน และแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง ให้สำนักงานโดยความเห็นชอบของ กกม.จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นนโยบาย มาตรฐาน และแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ”

มาตรา ๒๒ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๔๕ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๔๕ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ ตามนโยบาย มาตรฐาน และแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย”

มาตรา ๒๓ ให้ยกเลิกความในมาตรา ๔๘ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๔๘ โครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นกิจการที่มีความสำคัญต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความปลอดภัยสาธารณะและความสงบเรียบร้อยภายในประเทศ และให้สำนักงานมีหน้าที่ในการสนับสนุนและให้ความช่วยเหลือในการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ โดยเฉพาะที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ”

มาตรา ๒๔ ให้เพิ่มความต่อไปนี้เป็น (๗/๑) ในวรรคหนึ่ง ของมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“(๗/๑) ด้านอุตสาหกรรม”

มาตรา ๒๕ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๔๙/๑ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“มาตรา ๔๙/๑ ในกรณีที่คณะรัฐมนตรีหรือคณะกรรมการได้มอบหมายให้หน่วยงานภารกิจพิเศษดำเนินการใด โดยกำหนดให้สำนักงานต้องให้ความช่วยเหลือในการรักษาความมั่นคงปลอดภัยไซเบอร์ และในการดำเนินการนั้นมีความเสี่ยงที่ภัยคุกคามทางไซเบอร์หรือเหตุภัยคุกคามทางไซเบอร์จะเกิดขึ้น อันส่งผลหรืออาจส่งผลกระทบต่อความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ ความมั่นคงทางเศรษฐกิจ และความปลอดภัยสาธารณะหรือความสงบเรียบร้อยภายในประเทศ ให้หน่วยงานภารกิจพิเศษมีหน้าที่ดำเนินการป้องกันหรือลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่ กกม. กำหนด”

มาตรา ๒๖ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๕๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๕๐ ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ เพื่อประสานงานและเฝ้าระวังภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ โดยจะกำหนดให้หน่วยงานของรัฐที่มีความพร้อม หรือหน่วยงานควบคุมหรือกำกับดูแลที่มีหน้าที่กำกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ๆ ทำหน้าที่ดังกล่าวให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ทั้งหมดหรือบางส่วนก็ได้”

มาตรา ๒๗ ให้ยกเลิกความในวรรคสองของมาตรา ๕๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“เมื่อได้รับคำร้องเรียนตามวรรคหนึ่ง หาก กกม. พิจารณาแล้วเห็นว่า มีเหตุดังกล่าวและอาจทำให้เกิดภัยคุกคามทางไซเบอร์หรือเหตุภัยคุกคามทางไซเบอร์ ให้ กกม. ดำเนินการ ดังต่อไปนี้

(๑) กรณีเป็นหน่วยงานของรัฐ ให้แจ้งต่อผู้บริหารระดับสูงสุดของหน่วยงานเพื่อใช้อำนาจในทางบริหารสั่งการไปยังหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว

(๒) กรณีเป็นหน่วยงานเอกชน ให้แจ้งไปยังผู้บริหารระดับสูงสุดของหน่วยงาน ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว”

มาตรา ๒๘ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๕๔/๑ มาตรา ๕๔/๒ และมาตรา ๕๔/๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“มาตรา ๕๔/๑ เมื่อปรากฏแก่สำนักงานหรือมีเหตุอันควรเชื่อได้ว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่ปฏิบัติตามมาตรฐานที่คณะกรรมการหรือ กกม. กำหนด หรือไม่ปฏิบัติตามพระราชบัญญัตินี้ ให้สำนักงานมีอำนาจเข้าตรวจสอบการดำเนินงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ การตรวจสอบให้เป็นไปตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่คณะกรรมการกำหนด โดยคำนึงถึงความจำเป็นและไม่ก่อให้เกิดภาระแก่ผู้ถูกตรวจสอบเกินสมควร

มาตรา ๕๔/๒ ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใช้บริการจากผู้ให้บริการภายนอก ไม่ว่าจะเป็นบริการที่เป็นส่วนหนึ่งของระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศของหน่วยงานเอง หรือเป็นบริการที่สนับสนุนการดำเนินงานของระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศของหน่วยงาน ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าวมีหน้าที่กำกับและติดตามผู้ให้บริการภายนอก เพื่อให้ผู้ให้บริการภายนอกดังกล่าวดำเนินการตามมาตรฐานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่คณะกรรมการหรือ กกม. กำหนด หรือดำเนินการให้เป็นไปตามบทบัญญัติแห่งพระราชบัญญัตินี้

มาตรา ๕๔/๓ ในกรณีที่ปรากฏต่อสำนักงานว่าผู้ให้บริการภายนอกตามมาตรา ๕๔/๒ รายใดไม่ดำเนินการตามมาตรฐานที่คณะกรรมการหรือ กกม. กำหนดหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ ให้สำนักงานแจ้งเตือนให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกำกับให้ผู้ให้บริการภายนอกรายนั้นแก้ไขและดำเนินการให้สอดคล้องกับมาตรฐานหรือปฏิบัติตามพระราชบัญญัตินี้ ภายในหกสิบวันนับจากวันที่ได้รับหนังสือแจ้งเตือนจากสำนักงาน เมื่อครบกำหนดหกสิบวันดังกล่าวแล้ว ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศรายงานผลการดำเนินการต่อสำนักงานโดยเร็ว ในการนี้ หากผู้ให้บริการภายนอกดังกล่าวยังไม่ดำเนินการให้ถูกต้อง ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศพิจารณายุติการใช้บริการจากผู้ให้บริการรายดังกล่าวและแจ้งให้สำนักงานทราบ

ให้สำนักงานแจ้งรายชื่อผู้ให้บริการภายนอกที่ไม่ดำเนินการตามมาตรฐานที่คณะกรรมการหรือ กกม. กำหนดหรือไม่ปฏิบัติตามพระราชบัญญัตินี้ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบ และปรับปรุงรายชื่อให้เป็นปัจจุบันอยู่เสมอ เพื่อเป็นการป้องกันการใช้บริการจากผู้ให้บริการที่ไม่ดำเนินการให้เป็นไปตามมาตรฐานหรือให้เป็นไปตามพระราชบัญญัตินี้”

มาตรา ๒๙ ให้ยกเลิกความในมาตรา ๕๖ มาตรา ๕๗ และมาตรา ๕๘ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๕๖ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตนตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานตามมาตรา ๑๓ วรรคหนึ่ง (๔) รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการหรือ กกม. กำหนด และต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับเหตุภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

มาตรา ๕๗ ระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องดำเนินการใดอันเป็นการป้องกันหรือลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ ตามพระราชบัญญัตินี้ ให้รวมถึงระบบสารสนเทศที่อยู่ในความครอบครองของหน่วยงานโครงสร้างพื้นฐานทั้งในราชอาณาจักรและนอกราชอาณาจักร

มาตรา ๕๘ เมื่อมีเหตุอันควรเชื่อได้ว่าเกิดเหตุภัยคุกคามทางไซเบอร์ขึ้นต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือหน่วยงานเอกชน ให้หน่วยงานดังกล่าวดำเนินการตรวจสอบคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดเหตุภัยคุกคาม

ทางไซเบอร์ ให้หน่วยงานดำเนินการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ ตามนโยบาย มาตรฐาน และแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น”

มาตรา ๓๐ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๕๘/๑ มาตรา ๕๘/๒ และมาตรา ๕๘/๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“มาตรา ๕๘/๑ ในกรณีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตรวจสอบแล้วพบว่ามีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นต่อระบบสารสนเทศของตนที่เกี่ยวข้องกับภารกิจหรือบริการตามมาตรา ๔๙ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นรายงานข้อมูลไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตน

มาตรา ๕๘/๒ ในกรณีปรากฏต่อสำนักงานว่ามีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นต่อระบบสารสนเทศที่ไม่เกี่ยวข้องกับภารกิจหรือบริการตามมาตรา ๔๙ ของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือหน่วยงานเอกชนที่คณะกรรมการประกาศกำหนด ให้ดำเนินการดังต่อไปนี้

(๑) กรณีเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นก่อให้เกิดผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สำนักงานแจ้งหน่วยงานให้รายงานข้อมูลไปยังสำนักงาน

(๒) กรณีเหตุภัยคุกคามทางไซเบอร์อื่นที่มิใช่กรณีตาม (๑) หน่วยงานจะรายงานข้อมูลไปยังสำนักงานก็ได้

มาตรา ๕๘/๓ การรายงานตามมาตรา ๕๘/๑ และมาตรา ๕๘/๒ ให้เป็นตามหลักเกณฑ์ ระยะเวลา และวิธีการที่ กกม. กำหนด ทั้งนี้ การรายงานข้อมูลเบื้องต้นให้กระทำโดยผู้ที่มีหลักฐานว่าได้รับมอบอำนาจจากหน่วยงานหรือบุคคลที่หน่วยงานแจ้งต่อสำนักงานตามมาตรา ๔๖ และจะกระทำโดยทางโทรศัพท์ วิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใดที่สำนักงานกำหนดก็ได้

ในกรณีที่หน่วยงานหรือบุคคลใดพบอุปสรรคหรือปัญหาในการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ของตน หน่วยงานหรือบุคคลนั้นอาจร้องขอความช่วยเหลือไปยังสำนักงาน”

มาตรา ๓๑ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๕๙/๑ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“มาตรา ๕๙/๑ สำนักงาน หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานตามมาตรา ๕๐ อาจบันทึก ใช้หรือเปิดเผยข้อมูลที่ได้รับจากการรายงานตามมาตรา ๕๘/๑ หรือมาตรา ๕๘/๒ ได้เฉพาะเพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ และในกรณีดังต่อไปนี้

(๑) ให้การช่วยเหลือหน่วยงานเจ้าของระบบสารสนเทศที่ได้รับผลกระทบ รวมทั้งบุคคลหรือหน่วยงานที่ได้รับมอบหมายหรือที่ปฏิบัติการแทนหน่วยงานเจ้าของระบบสารสนเทศที่ได้รับผลกระทบ

(๒) ดำเนินการอื่นที่คณะกรรมการประกาศกำหนด

การบันทึก ใช้ หรือเปิดเผยข้อมูลตามวรรคหนึ่ง ต้องไม่ขัดต่อกฎหมายว่าด้วยคุ้มครองข้อมูลส่วนบุคคล และต้องไม่ใช้เพื่อประโยชน์ในการสืบสวนหรือลงโทษแก่หน่วยงานเจ้าของระบบสารสนเทศ

ที่ได้รับผลกระทบหรือหน่วยงานที่เกี่ยวข้องเนื่องจากการฝ่าฝืนหรือไม่ปฏิบัติตามบทบัญญัติแห่งกฎหมายอื่น เว้นแต่บทบัญญัติแห่งกฎหมายอื่นนั้นมีโทษทางอาญา”

มาตรา ๓๒ ให้ยกเลิกความในมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๖๐ ในการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ ให้แบ่งเหตุภัยคุกคามทางไซเบอร์เป็นสามระดับ ดังต่อไปนี้

(๑) เหตุภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง เหตุภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญที่จะก่อผลกระทบในระดับที่ทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยหรืออาจด้อยประสิทธิภาพลง

(๒) เหตุภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง เหตุภัยคุกคามทางไซเบอร์ที่มีลักษณะการเพิ่มขึ้นของผลกระทบอย่างมีนัยสำคัญจากการโจมตีคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศ และการโจมตีดังกล่าวมีผลทำให้หรืออาจทำให้ระบบคอมพิวเตอร์ หรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหายจนไม่สามารถทำงานหรือให้บริการได้

(๓) เหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง เหตุภัยคุกคามทางไซเบอร์ที่มีลักษณะ ดังต่อไปนี้

(ก) เป็นเหตุภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าเหตุภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลหรืออาจส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือโครงสร้างพื้นฐานสำคัญของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิต หรือคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) เป็นเหตุภัยคุกคามทางไซเบอร์ที่ก่อหรืออาจก่อให้เกิดผลกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

แผนการรับมือเหตุภัยคุกคามทางไซเบอร์ในแต่ละระดับตามวรรคหนึ่งให้เป็นไปตามที่คณะกรรมการประกาศกำหนด”

มาตรา ๓๓ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๖๐/๑ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“มาตรา ๖๐/๑ เมื่อปรากฏแก่ กกม. ว่าเกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ ให้ กกม. พิจารณา วิเคราะห์สถานการณ์ และประเมินผลกระทบที่เกิดหรือคาดว่าจะเกิดจากเหตุภัยคุกคามทางไซเบอร์ดังกล่าว เพื่อกำหนดระดับของเหตุภัยคุกคามทางไซเบอร์ตามมาตรา ๖๐ และให้ดำเนินการดังต่อไปนี้

(๑) ในกรณีเป็นเหตุภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง ให้ กกม. กำหนดมาตรการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ หรือรับมือเหตุภัยคุกคามทางไซเบอร์ ให้แก่หน่วยงานที่เกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ ดำเนินการ

(๒) ในกรณีเป็นเหตุภัยคุกคามทางไซเบอร์ระดับร้ายแรง ให้ดำเนินการตามมาตรา ๖๑ ถึงมาตรา ๖๖

(๓) ในกรณีเป็นเหตุภัยคุกคามทางไซเบอร์ระดับวิกฤต ให้ดำเนินการตามมาตรา ๖๗ และมาตรา ๖๘”

มาตรา ๓๔ ให้ยกเลิกความในมาตรา ๖๑ และมาตรา ๖๒ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๖๑ เมื่อปรากฏแก่ กกม. ว่าเกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ให้ กกม. ออกคำสั่งให้สำนักงานดำเนินการ ดังต่อไปนี้

(๑) รวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้องเพื่อวิเคราะห์สถานการณ์และประเมินผลกระทบจากเหตุภัยคุกคามทางไซเบอร์

(๒) สนับสนุน ให้ความช่วยเหลือ และเข้าร่วมในการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๓) ดำเนินการป้องกันเหตุภัยคุกคามทางไซเบอร์ เสนอแนะหรือสั่งการให้ใช้ระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการหาแนวทางตอบโต้หรือการแก้ไขปัญหาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๔) สนับสนุน ให้สำนักงาน และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ให้ความช่วยเหลือและเข้าร่วมในการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๕) แจ้งเตือนเหตุภัยคุกคามทางไซเบอร์ให้ทราบโดยทั่วกัน ทั้งนี้ ตามความจำเป็นและเหมาะสมโดยคำนึงถึงสถานการณ์ ความร้ายแรง และผลกระทบจากเหตุภัยคุกคามทางไซเบอร์นั้น

(๖) ให้ความสะดวกในการประสานงานระหว่างหน่วยงานของรัฐที่เกี่ยวข้องและหน่วยงานเอกชน เพื่อจัดการความเสี่ยงและรับมือเหตุภัยคุกคามทางไซเบอร์

มาตรา ๖๒ ในการดำเนินการตามมาตรา ๖๑ เพื่อประโยชน์ในการวิเคราะห์สถานการณ์และประเมินผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ ให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่ดำเนินการ ดังต่อไปนี้

(๑) มีหนังสือแจ้งให้บุคคลที่เกี่ยวข้องเพื่อมาให้ข้อมูลภายในระยะเวลาที่เหมาะสมและตามสถานที่ที่กำหนด หรือให้ข้อมูลเป็นหนังสือเกี่ยวกับเหตุภัยคุกคามทางไซเบอร์

(๒) มีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสารซึ่งอยู่ในความครอบครองของผู้อื่นอันเป็นประโยชน์แก่การดำเนินการ

(๓) สอบถามบุคคลผู้มีความรู้ความเข้าใจเกี่ยวกับข้อเท็จจริงและสถานการณ์ที่มีความเกี่ยวพันกับเหตุภัยคุกคามทางไซเบอร์

(๔) เข้าไปในอสังหาริมทรัพย์หรือสถานประกอบการที่เกี่ยวข้องหรือคาดว่ามีส่วนเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ของบุคคลหรือหน่วยงานที่เกี่ยวข้อง ทั้งนี้ การเข้าไปในอสังหาริมทรัพย์หรือสถานประกอบการดังกล่าว ให้กระทำระหว่างเวลาพระอาทิตย์ขึ้นและพระอาทิตย์ตก หรือในระหว่างเวลาทำการของสถานที่นั้น เว้นแต่มีเหตุอันควรเชื่อได้ว่าหากปล่อยเนิ่นช้าไปจะกระทบต่อการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ ให้เข้าไปในเวลากลางคืนหรือนอกเวลาทำการของสถานที่นั้นได้

(๕) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ รวมถึงถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ทำการถอดรหัสลับหรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

ผู้ให้ข้อมูลตามวรรคหนึ่ง ซึ่งกระทำโดยสุจริตย่อมได้รับการคุ้มครอง และไม่ถือว่าเป็นการละเมิดหรือผิดสัญญา

การใช้อำนาจของพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (๔) และ (๕) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าเกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับร้ายแรง บุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันควรเชื่อได้ว่าเกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ลักษณะของการกระทำ ตลอดจนรายละเอียดเกี่ยวกับอุปกรณ์ที่เกี่ยวข้องเท่าที่สามารถจะระบุได้ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว และเมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามวรรคหนึ่ง (๔) หรือ (๕) มอบให้เจ้าของหรือผู้ครอบครองอสังหาริมทรัพย์หรือสถานประกอบการหรือเจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์นั้นไว้เป็นหลักฐาน ในการนี้ ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามวรรคหนึ่ง (๔) หรือ (๕) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน”

มาตรา ๓๕ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๖๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๖๓ ในกรณีที่มีความจำเป็นเพื่อการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ ให้ กกม. มีคำสั่งให้หน่วยงานของรัฐให้ข้อมูล สนับสนุนบุคลากรในสังกัด หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์”

มาตรา ๓๖ ให้ยกเลิกความมาตรา ๖๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๖๔ ในกรณีที่เกิดหรือคาดว่าจะเกิดเหตุภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง ให้ กกม. ดำเนินการป้องกัน ลดความเสี่ยง หรือรับมือเหตุภัยคุกคามทางไซเบอร์ และดำเนินมาตรการที่จำเป็น

ในการดำเนินการตามวรรคหนึ่ง ให้ กกม. มีหนังสือถึงหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือถึงบุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องหรือได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ ให้ดำเนินมาตรการป้องกันโดยแก้ไขข้อบกพร่อง กำจัดชุดคำสั่งไม่พึงประสงค์หรือสกัดกั้นช่องทางการโจมตี หรือใช้มาตรการอื่นใด เพื่อลดความเสี่ยงของการเกิดเหตุภัยคุกคามทางไซเบอร์ที่คาดว่าจะเกิดขึ้น หรือให้กระทำการหรือระงับการดำเนินการใด ๆ เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงรับมือเหตุภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมและมีประสิทธิภาพตามแนวทางที่ กกม. กำหนด รวมทั้งร่วมกันบูรณาการในการดำเนินการเพื่อควบคุม ระงับ หรือบรรเทาผลที่เกิดจากเหตุภัยคุกคามทางไซเบอร์นั้นได้อย่างทันท่วงที ในการนี้ให้พนักงานเจ้าหน้าที่มีคำสั่งหรือดำเนินการใดเท่าที่จำเป็นเพื่อให้เป็นไปตามแนวทางที่ กกม. กำหนด

ให้เลขาธิการรายงานการดำเนินการตามมาตรานี้ต่อ กกม. อย่างต่อเนื่อง และเมื่อความเสี่ยงจากเหตุภัยคุกคามทางไซเบอร์ดังกล่าวสิ้นสุดลง ให้รายงานผลการดำเนินการต่อ กกม. โดยเร็ว”

มาตรา ๓๗ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๖๕ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๖๕ ในการรับมือและบรรเทาความเสียหายจากเหตุภัยคุกคามทางไซเบอร์ในระดับร้ายแรง รวมถึงเพื่อป้องกันหรือลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ ให้ กกม. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องหรือได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ดำเนินการ ดังต่อไปนี้

(๑) เฝ้าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง

(๒) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากเหตุภัยคุกคามทางไซเบอร์

(๓) ดำเนินมาตรการแก้ไขเหตุภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ที่ยังคงดำเนินอยู่

(๔) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(๕) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อรับมือเหตุภัยคุกคามทางไซเบอร์หรือลดความเสี่ยงของการเกิดเหตุภัยคุกคามทางไซเบอร์”

มาตรา ๓๘ ให้ยกเลิกความในมาตรา ๖๖ มาตรา ๖๗ มาตรา ๖๘ และมาตรา ๖๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๖๖ ในการรับมือเหตุภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ให้ กกม. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันหรือลดความเสี่ยงของการเกิดเหตุภัยคุกคามทางไซเบอร์ ในเรื่องดังต่อไปนี้

(๑) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องหรือได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์

(๒) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนาหรือสกัดคัดกรองข้อมูลสารสนเทศหรือข้อมูลคอมพิวเตอร์ รวมทั้งระงับการเผยแพร่ข้อมูลคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์

(๓) ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้อง หรือได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น

(๔) ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็นซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับเหตุภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบหรือวิเคราะห์ ทั้งนี้ ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าวให้ส่งคืนคอมพิวเตอร์หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์

ในการดำเนินการตาม (๑) ให้กระทำระหว่างเวลาพระอาทิตย์ขึ้นและพระอาทิตย์ตก หรือในระหว่างเวลาทำการของสถานที่นั้น เว้นแต่มีเหตุอันควรเชื่อได้ว่าหากปล่อยเนิ่นช้าไปจะกระทบต่อการป้องกัน ลดความเสี่ยงหรือรับมือเหตุภัยคุกคามทางไซเบอร์ ให้เข้าไปในเวลากลางคืนหรือนอกเวลาทำการของสถานที่นั้นได้

ในการดำเนินการตาม (๒) (๓) และ (๔) ให้ กกม. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดเหตุภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉิน และให้ศาลพิจารณาไต่สวนโดยเร็ว

มาตรา ๖๗ ในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง

มาตรา ๖๘ ในกรณีที่เป็นเหตุจำเป็นเร่งด่วน และเป็นเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติ คณะกรรมการอาจมอบหมายให้เลขาธิการมีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็น เพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้โดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากการดำเนินการดังกล่าว ให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว

ในกรณีเป็นเหตุภัยคุกคามทางไซเบอร์ในระดับร้ายแรงหรือวิกฤติ ให้เลขาธิการโดยความเห็นชอบของคณะกรรมการหรือ กกม. มีอำนาจขอข้อมูลที่เป็นปัจจุบันและต่อเนื่องจากผู้ที่เกี่ยวข้องกับเหตุภัยคุกคามทางไซเบอร์ โดยผู้นั้นต้องให้ความร่วมมือและให้ความสะดวกแก่คณะกรรมการหรือ กกม. โดยเร็ว

มาตรา ๖๙ ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับเหตุภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่งได้เฉพาะที่เป็นเหตุภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงเท่านั้น”

มาตรา ๓๙ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๖๙/๑ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“มาตรา ๖๙/๑ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญา มีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้

ในการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีผู้กระทำความผิดตามพระราชบัญญัตินี้ บรรดาที่เป็นอำนาจของพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ หรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ให้พนักงานเจ้าหน้าที่ประสานงานกับพนักงานสอบสวนผู้รับผิดชอบเพื่อดำเนินการตามอำนาจหน้าที่ต่อไป

ให้รัฐมนตรีมีอำนาจกำหนดระเบียบเกี่ยวกับแนวทางและวิธีปฏิบัติในการดำเนินการตามวรรคสอง”

มาตรา ๔๐ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๗๒/๑ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“มาตรา ๗๒/๑ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่ดำเนินการให้เป็นไปตามคำสั่งของ กกม. ที่ให้แก้ไขตามมาตรา ๕๓ วรรคสอง หรือมาตรา ๕๕ วรรคสอง แล้วแต่กรณี ต้องระวางโทษปรับไม่เกินสองแสนบาท”

มาตรา ๔๑ ให้ยกเลิกความในมาตรา ๗๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และให้ใช้ความต่อไปนี้แทน

“มาตรา ๗๓ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือหน่วยงานเอกชนใด ไม่รายงานเหตุภัยคุกคามทางไซเบอร์ตามมาตรา ๕๘/๑ หรือมาตรา ๕๘/๒ (๑) แล้วแต่กรณี โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท”

มาตรา ๔๒ ให้เพิ่มความต่อไปนี้เป็นวรรคสองของมาตรา ๗๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“ผู้ใดไม่ปฏิบัติตามคำสั่งของศาลหรือพนักงานเจ้าหน้าที่ที่สั่งตามมาตรา ๖๒ (๔) หรือ (๕) ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ”

มาตรา ๔๓ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๗๔/๑ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“มาตรา ๗๔/๑ ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งหรือขัดขวางการดำเนินการของพนักงานเจ้าหน้าที่ตามมาตรา ๖๔ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท และปรับอีกไม่เกินวันละหนึ่งหมื่นบาทนับแต่วันที่ครบกำหนดระยะเวลาที่พนักงานเจ้าหน้าที่ออกคำสั่งจนกว่าจะปฏิบัติให้ถูกต้อง”

มาตรา ๔๔ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๗๖/๑ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“มาตรา ๗๖/๑ ถ้าการกระทำความผิดตามมาตรา ๗๒/๑ มาตรา ๗๔ มาตรา ๗๔/๑ มาตรา ๗๕ และมาตรา ๗๖ เป็นเหตุให้เกิดเหตุภัยคุกคามทางไซเบอร์ หรือเกิดความเสียหายเพิ่มเติมหรือรุนแรงยิ่งขึ้น ซึ่งหากปฏิบัติตามคำสั่งของศาล กกม. หรือพนักงานเจ้าหน้าที่ แล้วแต่กรณี จะป้องกันการเกิดเหตุภัยคุกคามทางไซเบอร์หรือจะบรรเทาความเสียหายที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ได้ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท”

มาตรา ๔๕ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๗๗/๑ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“มาตรา ๗๗/๑ บรรดาความผิดอาญาตามหมวดนี้ เว้นแต่ความผิดตามมาตรา ๗๐ มาตรา ๗๖ และมาตรา ๗๖/๑ ให้คณะกรรมการเปรียบเทียบที่ กกม. แต่งตั้งมีอำนาจเปรียบเทียบได้

คณะกรรมการเปรียบเทียบตามวรรคหนึ่งให้มีจำนวนไม่เกินห้าคนซึ่งคนหนึ่งต้องเป็นพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

เมื่อคณะกรรมการเปรียบเทียบได้ทำการเปรียบเทียบกรณีใดและผู้ต้องหาได้ชำระเงินค่าปรับตามคำเปรียบเทียบภายในระยะเวลาที่คณะกรรมการเปรียบเทียบกำหนดแล้ว ให้ถือว่าคดีนั้นเป็นอันเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา

ในกรณีที่ผู้ต้องหาไม่ชำระเงินค่าปรับภายในระยะเวลาที่กำหนด ให้เริ่มนับอายุความในการฟ้องคดีใหม่นับตั้งแต่วันที่ครบกำหนดระยะเวลาดังกล่าว”

ผู้รับสนองพระบรมราชโองการ

.....

นายกรัฐมนตรี