ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
และหน่วยงานควบคุมหรือกำกับดูแล
พ.ศ. ๒๕๖๗

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแล ต้องกำหนดมาตรฐานที่เหมาะสม เพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ เพื่อให้การปฏิบัติงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นไปอย่างเหมาะสมและมีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๑๓ วรรคหนึ่ง (๕) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับมติที่ประชุมคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในคราวการประชุมครั้งที่ ๒/๒๕๖๖ เมื่อวันที่ ๑๕ ธันวาคม ๒๕๖๖ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“กมช.” หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“กกม.” หมายความว่า คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“ประกาศประมวลแนวทางปฏิบัติ” หมายความว่า ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

ข้อ ๔ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ดังต่อไปนี้

(๑) ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามหลักเกณฑ์ที่กำหนดในประกาศประมวลแนวทางปฏิบัติและตามมาตรฐานที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดและดำเนินการตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. ประกาศกำหนด

(๒) จัดทำเอกสารดังต่อไปนี้ของหน่วยงานของตนให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. ประกาศกำหนด ตามหลักเกณฑ์ที่กำหนดในประกาศประมวลแนวทางปฏิบัติให้แล้วเสร็จภายในระยะเวลา ๑ ปีนับแต่วันที่ประกาศนี้มีผลใช้บังคับ

(ก) ประมวลแนวทางปฏิบัติ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และแผนการรับมือภัยคุกคามทางไซเบอร์

(ข) กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วยการระบุความเสี่ยงที่อาจจะเกิดขึ้น มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ และมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

(๓) จัดให้มีการทบทวนเพื่อปรับปรุงหรือแก้ไขเพิ่มเติมนโยบาย มาตรฐาน และประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อการปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน

(๔) ให้ความร่วมมือและมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ รวมถึงการปฏิบัติตามคำขอใด ๆ ของ กมช. กกม. และสำนักงาน โดยให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญของตนเพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์

(๕) แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ พร้อมด้วยข้อมูลการติดต่อที่สามารถติดต่อได้ในกรณีมีเหตุฉุกเฉินภายในระยะเวลาหกสิบนาที เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน และหน่วยงานควบคุมหรือกำกับดูแล ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงข้อมูล ให้แจ้งรายชื่อหรือข้อมูลการติดต่อที่เปลี่ยนแปลงให้สำนักงานและหน่วยงานควบคุมหรือกำกับดูแลทราบภายในระยะเวลา ๑๕ วันนับแต่วันที่มีการเปลี่ยนแปลง

(๖) แจ้งรายชื่อหน่วยงานภายในหรือบุคคลที่เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์และผู้ดูแลระบบคอมพิวเตอร์ พร้อมด้วยข้อมูลการติดต่อที่สามารถติดต่อได้ในกรณีมีเหตุฉุกเฉินภายในระยะเวลาหกสิบนาทีไปยังสำนักงาน หน่วยงานควบคุมหรือกำกับดูแล และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยบุคคลดังกล่าวต้องเป็นบุคคล ผู้ซึ่งรับผิดชอบในการบริหารงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงข้อมูล ให้แจ้งรายชื่อหรือข้อมูลการติดต่อที่เปลี่ยนแปลงให้สำนักงาน หน่วยงานควบคุมหรือกำกับดูแล และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ก่อนการเปลี่ยนแปลงล่วงหน้าไม่น้อยกว่า ๗ วัน เว้นแต่มีเหตุจำเป็นอันไม่อาจก้าวล่วงได้ให้แจ้งภายในระยะเวลา ๑๕ วันนับแต่วันที่มีการเปลี่ยนแปลง

การเปลี่ยนแปลงข้อมูลตามวรรคหนึ่งให้รวมถึงการดำเนินการที่มีผลเป็นการเปลี่ยนแปลงเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น การเปลี่ยนแปลงหน่วยงานต้นสังกัดของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การยุบหรือควบรวมกิจการ การเพิ่มหน่วยงานย่อยภายในหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๗) ดำเนินการตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่กำหนดในนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. ประกาศกำหนด โดยให้ครอบคลุมโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และนำนโยบายดังกล่าว มาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยที่ยอมรับได้ (Risk Appetite) และให้นำส่งระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงดังกล่าวให้หน่วยงานควบคุมหรือกำกับดูแลของตนรับทราบและให้ความเห็นชอบก่อนนำส่งสำนักงาน

(๘) จัดให้มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดทำขึ้นตาม (๗) อย่างน้อยปีละหนึ่งครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ความเสี่ยงมาตรฐานสากล อย่างมีนัยสำคัญ

(๙) จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่งครั้ง โดยต้องประกอบด้วยรายละเอียดตามที่กำหนดในข้อ ๑๘ องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของประกาศประมวลแนวทางปฏิบัติ และจัดทำผลสรุปรายงานการดำเนินการ แยกต่างหากจากรายงานการประเมินความเสี่ยงของหน่วยงาน และส่งผลสรุปรายงานการดำเนินการดังกล่าวต่อสำนักงานภายใน ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จ แต่ไม่เกินวันที่ ๓๑ มกราคมของปีถัดไป พร้อมส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย ทั้งนี้ ผลสรุปรายงานดังกล่าว สำนักงานต้องไม่เปิดเผยต่อหน่วยงานอื่นใด เว้นแต่เป็นกรณีที่มีกฎหมายกำหนดให้กระทำได้

(๑๐) จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งเป็นบุคลากรภายในหน่วยงานของตนหรือเป็นผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละหนึ่งครั้ง และจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายใน ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จแต่ไม่เกินวันที่ ๓๑ มกราคมของปีถัดไป พร้อมส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย ทั้งนี้ ขอบเขตของการตรวจสอบและกรณีที่รายงานการตรวจสอบระบุว่าการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่สอดคล้องกับหลักเกณฑ์

หรือมาตรฐานการปฏิบัติงาน ให้เป็นไปตามหลักเกณฑ์ที่กำหนดในข้อ ๑๗ องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประกาศประมวลแนวทางปฏิบัติ

(๑๑) กำหนดกลไก ขั้นตอนหรือกระบวนการเพื่อตรวจสอบหรือเฝ้าระวังภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตนตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามที่กำหนดในประกาศประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. หรือ กกม. กำหนด

(๑๒) จัดให้มีการทบทวนกลไก ขั้นตอนหรือกระบวนการตาม (๑๑) อย่างน้อยปีละหนึ่งครั้ง

(๑๓) เข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

(๑๔) ตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ รวมถึงพฤติกรรมแวดล้อมของตน ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่

(๑๕) ในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการต่อไปนี้

(ก) เก็บรักษาข้อมูลและพยานหลักฐานตามที่กำหนดในขั้นตอนที่ ๒ - การตรวจจับและวิเคราะห์ (Detection and Analysis) ของเอกสารแนบ ๓ แนวทางการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หัวข้อแผนการรับมือภัยคุกคามทางไซเบอร์ และแนวทางการจัดทำกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หัวข้อมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ท้ายประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(ข) แจ้งเหตุและส่งรายงานภัยคุกคามทางไซเบอร์ไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล ภายในระยะเวลาและปฏิบัติตามหลักเกณฑ์และวิธีการตามที่กำหนดในประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๕๗

(ค) ให้ความร่วมมือกับพนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในการปฏิบัติการตามมาตรา ๖๖ รวมถึงให้ความร่วมมือกับพนักงานเจ้าหน้าที่หรือเจ้าหน้าที่ที่เกี่ยวข้องในการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเกี่ยวกับภัยคุกคามทางไซเบอร์

(๑๖) จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด เพื่อให้แน่ใจได้ว่าบริการที่สำคัญของตนยังสามารถให้บริการต่อไปได้

(๑๗) จัดให้มีการฝึกซ้อมตามแผนความต่อเนื่องทางธุรกิจตาม (๑๖) อย่างน้อยปีละหนึ่งครั้ง เพื่อประเมินประสิทธิภาพต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๑๘) จัดทำรายงานประจำปี ส่งรายงานดังกล่าวให้สำนักงานและหน่วยงานควบคุมหรือกำกับดูแลภายในวันที่ ๓๑ มกราคมของปีถัดไป โดยรายงานต้องมีรายละเอียด ดังต่อไปนี้

(ก) ระบุจำนวนและลักษณะของเหตุการณ์ภัยคุกคามทางไซเบอร์ของตน ตามแบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี ที่กำหนดท้ายประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๕๗

(ข) วิเคราะห์สาเหตุหรือผลกระทบที่เกิดขึ้นจากภัยคุกคามไซเบอร์ทางไซเบอร์ที่เกิดขึ้น

(ค) ปัญหาและอุปสรรคในการดำเนินงาน

(ง) ข้อเสนอแนะต่าง ๆ ซึ่งรวมถึงข้อเสนอแนะเชิงนโยบาย

(๑๙) ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นหน่วยงานของรัฐ ให้หน่วยงานดังกล่าวร่วมมือ สนับสนุนหรือดำเนินการเพื่อให้มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สำหรับบริการในด้านตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙ หรือเมื่อยังไม่มีความพร้อมในการทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าวให้แจ้งเหตุขัดข้องให้หน่วยงานควบคุมหรือกำกับดูแลของตนทราบถึงเหตุผลที่ยังไม่พร้อมในการทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นไปตามหลักเกณฑ์ที่ กมช. ประกาศกำหนด

(๒๐) ให้ความร่วมมือหรือสนับสนุนแก่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะเรื่องการติดตามการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์และผลการตอบสนองและรับมือเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

(๒๑) ดำเนินการตามที่ กมช. หรือ กกม. มอบหมายหรือประกาศกำหนด หรือให้ความร่วมมือกับสำนักงานหรือหน่วยงานควบคุมหรือกำกับดูแลเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งส่งเอกสารที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่สำนักงานหรือหน่วยงานควบคุมหรือกำกับดูแลร้องขอ

ข้อ ๕ ให้หน่วยงานควบคุมหรือกำกับดูแล มีหน้าที่ดังต่อไปนี้

(๑) กำหนดมาตรฐานที่เหมาะสมในการรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน โดยต้องสอดคล้องและไม่ต่ำกว่ามาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนด

(๒) กำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน เฉพาะบริการที่เป็นภารกิจหรือให้บริการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Services) ตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙ ให้อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยที่ยอมรับได้ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นและเป็นไปตามมาตรฐานที่เหมาะสมตาม (๑) และมาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนดด้วย

(๓) ตรวจสอบการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน ให้เป็นไปตามมาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนด และจัดทำรายงานสรุปผลการตรวจสอบให้แก่สำนักงานภายใน ๓๐ วัน หลังกระบวนการตรวจสอบเสร็จสิ้น ทั้งนี้ ในการดำเนินการดังกล่าว ให้หน่วยงานควบคุมหรือกำกับดูแลแต่งตั้งกลุ่มบุคคลทำหน้าที่เป็นผู้ตรวจสอบอันประกอบไปด้วยหัวหน้าทีมผู้ตรวจสอบ (Lead Auditor) และผู้ตรวจสอบ (Auditor) ที่มีความรู้ความเชี่ยวชาญด้านการตรวจสอบเรื่องความมั่นคงปลอดภัยไซเบอร์ ในกรณีที่พบว่าการดำเนินการไม่เป็นไปตามมาตรฐานขั้นต่ำที่ กมช. ประกาศกำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้งหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแก้ไขให้ได้มาตรฐาน พร้อมทั้งกำหนดเวลาให้ดำเนินการหากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ดำเนินการภายในระยะเวลาที่กำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้ง กกม. เพื่อดำเนินการตามมาตรา ๕๓ วรรคสอง ต่อไป

(๔) ให้ความช่วยเหลือ สนับสนุน หรือประสานงานในการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน

เมื่อมีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในด้านตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙ ด้านใดแล้ว ให้หน่วยงานควบคุมหรือกำกับดูแลแจ้งการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในด้านดังกล่าว พร้อมกับรายชื่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การดูแลและข้อมูลอื่น ๆ ที่เกี่ยวข้อง ให้สำนักงานทราบภายใน ๓๐ วันนับแต่วันที่จัดตั้ง

(๕) ให้ความช่วยเหลือ สนับสนุน หรือประสานงานในการประเมินความเสี่ยง ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของตน

(๖) ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และดำเนินการให้เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. ประกาศกำหนด

(๗) จัดทำเอกสารดังต่อไปนี้ของหน่วยงานของตนให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ กมช. ประกาศกำหนด ตามหลักเกณฑ์ที่กำหนดในประกาศประมวลแนวทางปฏิบัติให้แล้วเสร็จภายในระยะเวลา ๑ ปีนับแต่วันที่ประกาศนี้มีผลใช้บังคับ

(ก) ประมวลแนวทางปฏิบัติ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์

(ข) กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย การระบุความเสี่ยงที่อาจจะเกิดขึ้น มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ และมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

(๘) จัดให้มีการทบทวนเพื่อปรับปรุงหรือแก้ไขเพิ่มเติมนโยบาย มาตรฐานและประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่งคงปลอดภัยไซเบอร์ของหน่วยงานอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อการปฏิบัติการเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน

(๙) เข้าร่วมการดำเนินการ ประสานงาน และให้การสนับสนุน กกม. ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖

(๑๐) แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ พร้อมด้วยข้อมูลการติดต่อที่สามารถติดต่อได้ในกรณีมีเหตุฉุกเฉินภายในระยะเวลาหกสิบนาที เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงข้อมูล ให้แจ้งรายชื่อหรือข้อมูลการติดต่อที่เปลี่ยนแปลงให้สำนักงานทราบภายในระยะเวลา ๑๕ วัน นับแต่วันที่มีการเปลี่ยนแปลง

(๑๑) รับแจ้งและเก็บรักษาข้อมูลรายชื่อและข้อมูลการติดต่อของเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ และของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ที่ได้รับจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ปลอดภัย

(๑๒) เก็บรักษาข้อมูลที่จำเป็นของหน่วยงานที่ได้รับการแต่งตั้งหรือถูกยกเลิกจากการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๑๓) รับแจ้งข้อมูลจากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศภายใต้ที่อยู่ในการควบคุมหรือกำกับดูแลของตน และดำเนินการรวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และดำเนินการตามที่กำหนดในมาตรา ๕๙ เมื่อปรากฏภัยคุกคามทางไซเบอร์แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเกิดขึ้น

(๑๔) ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามหลักเกณฑ์ที่กำหนดในประกาศประมวลแนวทางปฏิบัติ และในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการต่อไปนี้ด้วย

(ก) เก็บรักษาข้อมูลและพยานหลักฐานตามที่กำหนดในขั้นตอนที่ ๒ - การตรวจจับและวิเคราะห์ (Detection and Analysis) ของเอกสารแนบ ๓ แนวทางการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หัวข้อแผนการรับมือภัยคุกคามทางไซเบอร์ และแนวทางการจัดทำกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หัวข้อมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ท้ายประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(ข) แจ้งเหตุไปยังสำนักงานภายในระยะเวลาและปฏิบัติตามหลักเกณฑ์และวิธีการตามที่กำหนดในประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๕๗

(ค) ให้ความร่วมมือกับพนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในการปฏิบัติการตามมาตรา ๖๖ รวมถึงให้ความร่วมมือกับพนักงานเจ้าหน้าที่หรือเจ้าหน้าที่อื่นที่เกี่ยวข้องในการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเกี่ยวกับภัยคุกคามทางไซเบอร์

(๑๕) รับทราบและให้ความเห็นหรือข้อเสนอแนะเกี่ยวกับระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำก่อนส่งให้แก่สำนักงาน

(๑๖) จัดทำรายงานประจำปี และส่งรายงานดังกล่าวให้สำนักงาน ภายในวันที่ ๓๑ มกราคมของปีถัดไป โดยรายงานต้องมีรายละเอียดดังต่อไปนี้

(ก) ระบุจำนวนและลักษณะของเหตุการณ์ภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน ตามแบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี ที่กำหนดท้ายประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๕๗

(ข) วิเคราะห์สาเหตุหรือผลกระทบที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(ค) ปัญหาและอุปสรรคในการดำเนินงาน

(ง) ข้อเสนอแนะต่าง ๆ ซึ่งรวมถึงข้อเสนอแนะเชิงนโยบาย

หากหน่วยงานเป็นทั้งหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีภารกิจหรือการให้บริการตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙ ให้จัดทำรายงานโดยรวมข้อมูลของตนในบทบาทที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้วย

(๑๗) ให้ความช่วยเหลือหรือสนับสนุนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในควบคุมหรือกำกับดูแลของตน ในการจัดทำหรือปรับปรุงมาตรการป้องกัน รับมือ ปราบปรามและระงับภัยคุกคามทางไซเบอร์ ให้มีความเหมาะสมและเป็นปัจจุบัน และเก็บรักษาข้อมูลดังกล่าวให้ปลอดภัย

(๑๘) ให้ความช่วยเหลือหรือสนับสนุนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในควบคุมหรือกำกับดูแลของตน ในการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ และการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

(๑๙) ให้ความร่วมมือ สนับสนุนหรือดำเนินการเพื่อให้มีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในด้านของตนตามประกาศที่ออกโดยอาศัยอำนาจตามมาตรา ๔๙

ในกรณีที่ไม่มีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่เป็นหน่วยงานของรัฐใดมีความพร้อมและหน่วยงานกำกับหรือดูแลไม่พร้อมทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าวให้แจ้งเหตุขัดข้องให้สำนักงานทราบถึงเหตุผลที่ยังไม่พร้อมในการทำหน้าที่เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นไปตามหลักเกณฑ์ที่ กมช. ประกาศกำหนด

(๒๐) ให้ความร่วมมือหรือสนับสนุนแก่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ในการติดตามการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และผลการตอบสนองและรับมือเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

(๒๑) ประสานงาน ให้ความร่วมมือ หรือสนับสนุน แก่หน่วยงานควบคุมหรือกำกับดูแลอื่นเพื่อให้การควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีความสอดคล้องกัน

(๒๒) ดำเนินการตามที่ กมช. หรือ กกม. มอบหมายหรือประกาศกำหนด หรือให้ความร่วมมือกับสำนักงานหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๖ ให้สำนักงานพิจารณาทบทวนหน้าที่ของหน่วยงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานควบคุมหรือกำกับดูแลอย่างน้อยทุก ๒ ปี หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างมีนัยสำคัญ

ข้อ ๗ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์รักษาการตามประกาศนี้และให้มีอำนาจออกประกาศ คำสั่ง หลักเกณฑ์และวิธีการเพื่อปฏิบัติตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เป็นผู้มีอำนาจตีความและวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยของประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่สุด

ประกาศ ณ วันที่ ๕ กุมภาพันธ์ พ.ศ. ๒๕๖๗
ประเสริฐ จันทรรวงทอง
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์