

ระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
ว่าด้วยการมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๕

โดยที่เป็นการสมควรกำหนดให้มีระเบียบและหลักเกณฑ์เกี่ยวกับการมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ในการดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ระดับร้ายแรงได้ทันที

อาศัยอำนาจตามความในมาตรา ๑๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบมติที่ประชุมคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ครั้งที่ ๒/๒๕๖๕ เมื่อวันที่ ๑ สิงหาคม ๒๕๖๕ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ จึงออกระเบียบไว้ ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ว่าด้วยการมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในระเบียบนี้

“มอบอำนาจ” หมายความว่า การที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ มีหน้าที่และอำนาจที่จะพึงปฏิบัติ หรือดำเนินการตามกฎหมาย กฎ ระเบียบ ประกาศ หรือคำสั่งใด หรือมติของคณะรัฐมนตรีในเรื่องใด ได้มอบอำนาจในการสั่ง การอนุญาต การอนุมัติ การปฏิบัติการแทน หรือการดำเนินการอื่นใดตามกฎหมาย กฎ ระเบียบ ประกาศ หรือคำสั่งใด หรือมติของคณะรัฐมนตรี ในเรื่องนั้น ให้แก่คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงปฏิบัติการแทน

“ผู้มอบอำนาจ” หมายความว่า คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ที่มีอำนาจที่จะพึงปฏิบัติหรือดำเนินการตามกฎหมาย กฎ ระเบียบ ประกาศ หรือคำสั่งใด หรือมติของคณะรัฐมนตรี ในการสั่งการอนุญาต การอนุมัติ การปฏิบัติการแทน หรือการดำเนินการอื่นใด

“ผู้รับมอบอำนาจ” หมายความว่า คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หรือเลขาธิการ ที่ได้รับมอบอำนาจจากคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ที่มีอำนาจหน้าที่ดังกล่าว

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ประกาศกำหนดลักษณะ หน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง” หมายความว่า ภัยคุกคามที่มีลักษณะการเพิ่มขึ้น อย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมีเป้าหมาย เพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือ โครงสร้างพื้นฐานทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงาน หรือให้บริการได้

“กกม.” หมายความว่า คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

“คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง” หมายความว่า คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามที่คณะกรรมการกำกับดูแล ด้านความมั่นคงปลอดภัยไซเบอร์แต่งตั้งและมอบอำนาจให้ปฏิบัติการแทนตามระเบียบนี้

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

“เลขาธิการ” หมายความว่า เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ

“การประชุมผ่านสื่ออิเล็กทรอนิกส์” หมายความว่า การประชุมที่กฎหมายบัญญัติให้ต้อง มีการประชุมที่ได้กระทำผ่านสื่ออิเล็กทรอนิกส์ โดยผู้ร่วมประชุมมีได้อยู่ในสถานที่เดียวกันและสามารถ ประชุมปรึกษาหารือ และแสดงความคิดเห็นระหว่างกันได้ผ่านสื่ออิเล็กทรอนิกส์

“ผู้ร่วมประชุม” หมายความว่า ประธานกรรมการ กรรมการ หรือเลขานุการ ผู้ช่วยเลขานุการ และให้หมายความรวมถึงผู้ซึ่งต้องชี้แจงแสดงความคิดเห็นต่อคณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ ในระดับร้ายแรงนั้นด้วย

ข้อ ๔ เพื่อให้การดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ได้ทันทั่วทั้งที่ ให้คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์สามารถมอบอำนาจให้ คณะกรรมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หรือเลขาธิการได้ ตามมาตรา ๖๑

มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมทั้งปฏิบัติการตามระเบียบนี้

ข้อ ๕ ให้มี คณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรง” เรียกโดยย่อว่า “ครร.” ประกอบด้วย

- | | |
|---|-------------------------|
| (๑) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม | เป็นประธานกรรมการ |
| (๒) ผู้บัญชาการทหารสูงสุด | เป็นกรรมการ |
| (๓) ผู้บัญชาการตำรวจแห่งชาติ | เป็นกรรมการ |
| (๔) ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม | เป็นกรรมการ |
| (๕) เลขาธิการสภาความมั่นคงแห่งชาติ | เป็นกรรมการ |
| (๖) เลขาธิการ | เป็นกรรมการและเลขานุการ |

ให้เลขานุการแต่งตั้งพนักงานของสำนักงาน เป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

ข้อ ๖ เมื่อปรากฏแก่ ครร. หรือโดยการเสนอแนะของสำนักงาน ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ ครร. มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) ร่วมกันปฏิบัติการเพื่อรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรงกับหน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรการป้องกันรับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ตามประกาศคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกันรับมือ ประเมิน ปรามปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔”

(๒) ดูแลและดำเนินการเพื่อรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ดังนี้

(๒.๑) กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุนต่อคณะกรรมการเพื่อรับมือภัยคุกคามทางไซเบอร์ในระดับร้ายแรงได้อย่างทันที่

(๒.๒) มอบหมายให้สำนักงานวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ รวมทั้งการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์ เพื่อพิจารณาสั่งการ เมื่อมีหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง เพื่อประโยชน์ในการติดตามและตรวจสอบผลการดำเนินการดังกล่าว ให้สำนักงานรายงานผลการดำเนินการต่อ กกม. ทราบด้วย

(๒.๓) เมื่อปรากฏแก่ ครร. ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ ครร. ออกคำสั่งให้สำนักงานดำเนินการตามมาตรา ๖๑ เพื่อประโยชน์ในการวิเคราะห์สถานการณ์และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ และให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามมาตรา ๖๒

(๒.๔) ในกรณีที่มีความจำเป็นเพื่อป้องกัน รั้งมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้ ครร. มีคำสั่งให้หน่วยงานของรัฐให้ข้อมูล สนับสนุนบุคลากรในสังกัด หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ครร. ต้องดูแลมิให้มีการใช้ข้อมูลที่ได้มาตาม (๒.๔) วรรคหนึ่ง ในลักษณะที่อาจก่อให้เกิดความเสียหาย และเสนอให้ กกม. รับผิดชอบในค่าตอบแทนบุคลากร ค่าใช้จ่ายหรือความเสียหายที่เกิดขึ้นจากการใช้เครื่องมือทางอิเล็กทรอนิกส์ดังกล่าว

ให้นำความใน (๒.๔) วรรคหนึ่ง และวรรคสอง มาใช้บังคับในการร้องขอต่อเอกชน โดยความยินยอมของเอกชนนั้นด้วย

(๒.๕) ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง ให้ ครร. ดำเนินการป้องกัน รั้งมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และดำเนินมาตรการที่จำเป็น

ในการดำเนินการตาม (๒.๕) วรรคหนึ่ง ให้ ครร. มีหนังสือถึงหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กระทำการหรือระงับการดำเนินการใด ๆ เพื่อป้องกัน รั้งมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมและมีประสิทธิภาพ ตามแนวทางที่ กกม. กำหนด รวมทั้งร่วมกันบูรณาการในการดำเนินการเพื่อควบคุม ระงับ หรือบรรเทาผลที่เกิดจากภัยคุกคามทางไซเบอร์นั้นได้อย่างทันท่วงที

ให้เลขาธิการรายงานการดำเนินการตาม (๒.๕) วรรคหนึ่ง และวรรคสองนี้ต่อ กกม. อย่างต่อเนื่อง และเมื่อภัยคุกคามทางไซเบอร์ดังกล่าวสิ้นสุดลง ให้รายงานผลการดำเนินการต่อ กกม. โดยเร็ว

(๒.๖) ในการรั้งมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ให้ ครร. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของ กรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ ดำเนินการ ดังต่อไปนี้

(๒.๖.๑) ฝั่าระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใด ระยะเวลาหนึ่ง

(๒.๖.๒) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๒.๖.๓) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่อง หรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่

(๒.๖.๔) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(๒.๖.๕) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์

ในกรณีมีเหตุจำเป็นที่ต้องเข้าถึงข้อมูลตาม (๒.๖.๕) ให้ ครร. มอบหมายให้เลขานุการ ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครองผู้ใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ตาม (๒.๖) วรรคหนึ่งดำเนินการตามคำร้อง ทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่ง ที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

(๒.๗) ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ครร. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ในเรื่อง ดังต่อไปนี้

(๒.๗.๑) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(๒.๗.๒) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(๒.๗.๓) ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น

(๒.๗.๔) ยึดหรืออายัดคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์ใด ๆ เฉพาะเท่าที่จำเป็นซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ เพื่อการตรวจสอบหรือวิเคราะห์ ทั้งนี้ ไม่เกินสามสิบวัน เมื่อครบกำหนดเวลาดังกล่าวให้ส่งคืนคอมพิวเตอร์หรืออุปกรณ์ใด ๆ แก่เจ้าของกรรมสิทธิ์ หรือผู้ครอบครองโดยทันทีหลังจากเสร็จสิ้นการตรวจสอบหรือวิเคราะห์

ในการดำเนินการตาม (๒.๗.๒) (๒.๗.๓) และ (๒.๗.๔) ให้ ครร. มอบหมายให้เลขานุการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่ง ที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

(๓) ปฏิบัติการอื่นใดตามที่ กกม. มอบหมาย

ข้อ ๗ ในการนัดประชุมของ ครร. ให้เลขานุการแจ้งให้คณะกรรมการทุกคนทราบล่วงหน้าอย่างน้อยสามวัน โดยจะแจ้งด้วยวาจาก่อนและทำเป็นหนังสือ หรือโดยวิธีการทางอิเล็กทรอนิกส์ก็ได้ เว้นแต่จะได้มีการแจ้งกำหนดการนัดประชุมในที่ประชุมครั้งก่อนหน้าแล้ว

ในกรณีที่มีเหตุจำเป็นเร่งด่วนและไม่อาจนัดประชุมล่วงหน้าตามกำหนดเวลาในวรรคหนึ่งได้ ให้เลขานุการแจ้งให้ ครร. เพื่อนัดประชุมเป็นการเร่งด่วนได้ โดยให้นำวิธีการตามวรรคหนึ่งมาใช้ โดยอนุโลม ทั้งนี้ ให้บันทึกการแจ้งนัดประชุม ครร. แต่ละคนไว้เป็นหลักฐานด้วย

ให้เลขานุการจัดส่งระเบียบวาระการประชุมและเอกสารที่เกี่ยวข้องไปพร้อมกับหนังสือนัดประชุม หรือจะส่งโดยจดหมายอิเล็กทรอนิกส์ก็ได้ แต่ต้องมีมาตรการในการรักษาความปลอดภัยต่อเอกสารอิเล็กทรอนิกส์ดังกล่าวด้วย เว้นแต่กรณีที่มีเหตุจำเป็นอาจส่งหลังจากการแจ้งนัดประชุมหรือส่งในวันที่มีการประชุมก็ได้

ข้อ ๘ การกำหนดระเบียบวาระการประชุมของ ครร. อย่างน้อยต้องมีรายละเอียด ดังต่อไปนี้

(๑) เรื่องที่ประธานแจ้งต่อที่ประชุม

(๒) เรื่องรับรองรายงานการประชุม

(๓) เรื่องเสนอเพื่อทราบ

(๔) เรื่องที่ค้างพิจารณาหรือเรื่องสืบเนื่อง

(๕) เรื่องเสนอเพื่อพิจารณา

ข้อ ๙ การประชุมของ ครร. ให้ถือปฏิบัติ ดังต่อไปนี้

(๑) ต้องมี ครร. มาประชุมไม่น้อยกว่ากึ่งหนึ่งของจำนวน ครร. ทั้งหมดที่มีอยู่จึงจะเป็นองค์ประชุม

(๒) ให้ประธาน ครร. เป็นประธานในที่ประชุม ถ้าประธาน ครร. ไม่อยู่ในที่ประชุม หรือไม่สามารถปฏิบัติหน้าที่ได้ ให้ที่ประชุมเลือก ครร. คนหนึ่ง เพื่อทำหน้าที่เป็นประธานในที่ประชุม

(๓) ครร. ผู้ใดมีส่วนได้เสียโดยตรงในเรื่องที่จะพิจารณา ครร. ผู้นั้นไม่มีสิทธิเข้าร่วมประชุม และไม่มีสิทธิออกเสียงลงคะแนนในเรื่องนั้น แต่ให้นับเป็นองค์ประชุมด้วย

(๔) การวินิจฉัยชี้ขาดของที่ประชุมให้ถือเสียงข้างมาก ครร. คนหนึ่งให้มีเสียงหนึ่งในการลงคะแนน ถ้าคะแนนเสียงเท่ากัน ให้ประธานในที่ประชุมออกเสียงเพิ่มขึ้นอีกหนึ่งเสียงเป็นเสียงชี้ขาด

(๕) เรื่องใดที่ ครร. รับรองมติการประชุมแล้ว ให้เลขานุการแจ้งมติของที่ประชุมให้ผู้เกี่ยวข้องทราบโดยมิต้องรอการรับรองรายงานการประชุม

ข้อ ๑๐ กรรมการที่แต่งตั้งโดยตำแหน่ง ถ้าผู้ดำรงตำแหน่งนั้นไม่อาจเข้าประชุมได้ ผู้เข้าประชุมแทนซึ่งเป็นผู้มีอำนาจทำหน้าที่แทนตามกฎหมายและให้นับเป็นองค์ประชุม

ข้อ ๑๑ การประชุมผ่านสื่ออิเล็กทรอนิกส์ของ ครร. ให้เป็นไปตามกฎหมายว่าด้วยการประชุมผ่านสื่ออิเล็กทรอนิกส์

ข้อ ๑๒ ให้ ครร. ืบรายงานการดำเนินการดังกล่าวตามข้อ ๖ ต่อประธาน กกม. โดยด่วน และอย่างต่อเนื่อง และเมื่อภัยคุกคามทางไซเบอร์สิ้นสุดลง ให้รายงานผลการดำเนินการต่อ กกม. เพื่อทราบด้วย

ข้อ ๑๓ กำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุนต่อคณะกรรมการรับมือเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรงได้อย่างทันท่วงที

ข้อ ๑๔ ให้สำนักงานหรือพนักงานเจ้าหน้าที่ ประสานงานกับผู้เกี่ยวข้อง ในการดำเนินการตามหน้าที่และอำนาจตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ในการดำเนินการตามความวรรคหนึ่ง อาจทำเป็นหนังสือหรือวาจาหรือโดยการสื่อความหมายในรูปแบบอื่นก็ได้ แต่ต้องมีข้อความหรือความหมายที่ชัดเจนเพียงพอที่จะเข้าใจได้ ในกรณีที่สั่งการด้วยวาจา ถ้าผู้รับคำสั่งนั้นร้องขอและการร้องขอได้กระทำโดยมีเหตุอันสมควรภายในเจ็ดวัน นับแต่วันที่มีคำสั่งดังกล่าว เลขาธิการต้องยืนยันคำสั่งนั้นเป็นหนังสือ

ทั้งนี้ ให้รับรายงานต่อประธาน กกม. โดยด่วนและอย่างต่อเนื่อง และเมื่อภัยคุกคามทางไซเบอร์สิ้นสุดลง ให้รายงานผลการดำเนินการต่อ กกม. เพื่อทราบด้วย

ข้อ ๑๕ ในการปฏิบัติการแทนผู้รับมอบอำนาจอาจดำเนินการใด ๆ เพื่อให้บรรลุวัตถุประสงค์ของการมอบอำนาจนั้นตามที่เห็นสมควร แต่ต้องใช้อำนาจที่มอบให้เป็นไปตามกฎหมายที่เกี่ยวข้องกับเรื่องที่มีการมอบอำนาจหรือตามหลักเกณฑ์และเงื่อนไขการใช้อำนาจในเรื่องนั้น รวมทั้งต้องจัดทำรายงานผลการใช้อำนาจดังกล่าวตามหลักเกณฑ์ที่ผู้มอบอำนาจกำหนด

ข้อ ๑๖ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เป็นผู้รักษาการตามระเบียบนี้ และมีอำนาจออกประกาศ หรือคำสั่ง หลักเกณฑ์และวิธีการเพื่อประโยชน์ในการปฏิบัติตามระเบียบนี้

ในกรณีที่มีปัญหาเกี่ยวกับการบังคับใช้หรือการปฏิบัติตามระเบียบนี้ หรือระเบียบนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ มีอำนาจตีความและวินิจฉัยชี้ขาด ทั้งนี้ การตีความและคำวินิจฉัยของประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๑๓ กันยายน พ.ศ. ๒๕๖๕

ชัยวุฒิ ธนาคมานุสรณ์

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์