

ที่ สกมช ๐๐๐๑/๙๒

๑๔ มกราคม ๒๕๖๔

สำนักงาน ก.พ.ร.
รับที่ ๐๐๔๐๖
วันที่ 18 ม.ค. 2564
เวลา

เรื่อง ขอส่งคำขอจัดกลุ่มองค์การมหาชนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ

เรียน เลขาธิการ ก.พ.ร.

อ้างถึง หนังสือสำนักงาน ก.พ.ร. ที่ นร ๑๒๐๘/๖๓๗ ลงวันที่ ๖ กันยายน ๒๕๖๒

สิ่งที่ส่งมาด้วย ๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒. มติการประชุมคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย
ไซเบอร์ ครั้งที่ ๑/๒๕๖๓

๓. คำขอจัดกลุ่มองค์การมหาชนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย
ไซเบอร์แห่งชาติ

ตามหนังสือที่อ้างถึง สำนักงาน ก.พ.ร. ได้แจ้งว่าคณะกรรมการพัฒนาและส่งเสริมองค์การ
มหาชน (กพม.) ในการประชุมครั้งที่ ๒/๒๕๖๒ เมื่อวันที่ ๑๖ สิงหาคม ๒๕๖๒ ได้พิจารณาและมีมติให้
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นองค์การมหาชนที่จัดตั้งตาม
พระราชบัญญัติเฉพาะตามมติคณะรัฐมนตรีเมื่อวันที่ ๒๐ ตุลาคม ๒๕๕๒ โดยแจ้งให้สำนักงานฯ ปฏิบัติตามมติ
คณะรัฐมนตรี และให้ส่งคำขอจัดกลุ่มองค์การมหาชนพร้อมข้อมูลประกอบการพิจารณา ได้แก่ วัตถุประสงค์
บทบาทภารกิจ องค์ประกอบคณะกรรมการบริหาร โครงสร้าง อัตรากำลัง ความยากง่ายหรือความยุ่งยาก
ซับซ้อนของภารกิจ และสมรรถนะของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ไปยังสำนักงาน ก.พ.ร. เพื่อขอจัดกลุ่ม ทั้งนี้ ในระหว่างที่ยังมิได้รับการจัดกลุ่มให้สำนักงานฯ เป็นองค์การ
มหาชนกลุ่ม ๓ (บริการสาธารณะทั่วไป) ไปพลางก่อน นั้น

คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ ในคราว
การประชุมครั้งที่ ๑/๒๕๖๓ เมื่อวันที่ ๘ กันยายน ๒๕๖๓ มีมติเห็นชอบในหลักการคำขอจัดกลุ่มองค์การมหาชน
ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในการนี้ สำนักงานคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์จึงขอส่งคำขอจัดกลุ่มองค์การมหาชนของสำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นองค์การมหาชนกลุ่ม ๑ รายละเอียดตามสิ่งที่ส่งมาด้วย ๑-๓ มายัง
สำนักงาน ก.พ.ร. เพื่อเสนอ กพม. และคณะรัฐมนตรีพิจารณาต่อไป

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

พลโท ดร.



(ปรัชญา เฉลิมวัฒน์)

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



พระราชบัญญัติ

การรักษาความมั่นคงปลอดภัยไซเบอร์

พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒

เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว
มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

พระราชบัญญัตินี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล
ซึ่งมาตรา ๒๖ ประกอบกับมาตรา ๒๘ มาตรา ๓๒ มาตรา ๓๓ มาตรา ๓๔ มาตรา ๓๖ และ
มาตรา ๓๗ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย บัญญัติให้กระทำได้โดยอาศัยอำนาจตามบทบัญญัติ
แห่งกฎหมาย

เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพของบุคคลตามพระราชบัญญัตินี้
เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และ
ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายใน
ประเทศ ซึ่งการตราพระราชบัญญัตินี้สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญ
แห่งราชอาณาจักรไทยแล้ว

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของ
สภานิติบัญญัติแห่งชาติทำหน้าที่รัฐสภา ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า “พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒”

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษา เป็นต้นไป

มาตรา ๓ ในพระราชบัญญัตินี้

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อย ภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้าย ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง

“ไซเบอร์” หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้ เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของ ดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

“หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์การฝ่ายนิติบัญญัติ องค์การฝ่ายตุลาการ องค์การอิสระ องค์การมหาชน และหน่วยงานอื่น ของรัฐ

“ประมวลแนวทางปฏิบัติ” หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแล ด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

“เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มีขอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัย ไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบ คอมพิวเตอร์

“มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า การแก้ไข ปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวข้องกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจ และเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

“โครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย ของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็น ประโยชน์สาธารณะ

“หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ” หมายความว่า หน่วยงานของรัฐหรือ หน่วยงานเอกชน ซึ่งมีการจัดหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“หน่วยงานควบคุมหรือกำกับดูแล” หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือ บุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของ หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

“คณะกรรมการ” หมายความว่า คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“เลขาธิการ” หมายความว่า เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

มาตรา ๔ ให้นายกรัฐมนตรีรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจออกประกาศ และแต่งตั้งพนักงานเจ้าหน้าที่ เพื่อปฏิบัติการตามพระราชบัญญัตินี้

ประกาศนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้

หมวด ๑

คณะกรรมการ

ส่วนที่ ๑

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๕ ให้มีคณะกรรมการคณะหนึ่งเรียกว่า “คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ” เรียกโดยย่อว่า “กมช.” และให้ใช้ชื่อเป็นภาษาอังกฤษว่า “National Cyber Security Committee” เรียกโดยย่อว่า “NCSC” ประกอบด้วย

(๑) นายกรัฐมนตรี เป็นประธานกรรมการ

(๒) กรรมการโดยตำแหน่ง ได้แก่ รัฐมนตรีว่าการกระทรวงกลาโหม รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงการคลัง ปลัดกระทรวงยุติธรรม ผู้บัญชาการตำรวจแห่งชาติ และเลขาธิการสภาความมั่นคงแห่งชาติ

(๓) กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินเจ็ดคน ซึ่งคณะรัฐมนตรีแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านการคุ้มครองข้อมูลส่วนบุคคล ด้านวิทยาศาสตร์ ด้านวิศวกรรมศาสตร์ ด้านกฎหมาย ด้านการเงิน หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

หลักเกณฑ์และวิธีการสรรหาบุคคลเพื่อเสนอคณะรัฐมนตรีแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิ รวมทั้งการสรรหากรรมการผู้ทรงคุณวุฒิเพื่อดำรงตำแหน่งแทนผู้ที่พ้นจากตำแหน่งก่อนวาระตามมาตรา ๗ วรรคสอง ให้เป็นไปตามระเบียบที่คณะรัฐมนตรีกำหนดโดยการเสนอแนะของคณะกรรมการ

มาตรา ๖ กรรมการผู้ทรงคุณวุฒิในคณะกรรมการต้องมีสัญชาติไทยและไม่มีลักษณะต้องห้าม ดังต่อไปนี้

(๑) เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต

(๒) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ

(๓) เคยต้องคำพิพากษาถึงที่สุดให้จำคุกไม่ว่าจะได้รับโทษจำคุกจริงหรือไม่ เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ

(๔) เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หรือออกจากงานจากหน่วยงานที่เคยปฏิบัติหน้าที่ เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง

(๕) เคยถูกถอดถอนออกจากตำแหน่งตามกฎหมาย

(๖) เป็นผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่นหรือผู้บริหารท้องถิ่น กรรมการหรือผู้ดำรงตำแหน่งซึ่งรับผิดชอบการบริหารพรรคการเมือง ที่ปรึกษาพรรคการเมือง หรือเจ้าหน้าที่ของพรรคการเมือง

มาตรา ๗ กรรมการผู้ทรงคุณวุฒิในคณะกรรมการมีวาระการดำรงตำแหน่งคราวละสี่ปี และอาจได้รับแต่งตั้งอีกได้ แต่จะดำรงตำแหน่งเกินสองวาระไม่ได้

ในกรณีที่มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งก่อนวาระ ให้ผู้ได้รับแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของกรรมการผู้ทรงคุณวุฒิซึ่งได้แต่งตั้งไว้แล้ว เว้นแต่วาระที่เหลืออยู่ไม่ถึงเก้าสิบวันจะไม่แต่งตั้งกรรมการผู้ทรงคุณวุฒิแทนก็ได้

เมื่อครบกำหนดวาระตามวรรคหนึ่ง หากยังมิได้แต่งตั้งกรรมการผู้ทรงคุณวุฒิขึ้นใหม่ ให้กรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าจะได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิขึ้นใหม่

มาตรา ๘ นอกจากการพ้นจากตำแหน่งตามวาระตามมาตรา ๗ กรรมการผู้ทรงคุณวุฒิพ้นจากตำแหน่ง เมื่อ

(๑) ตาย

(๒) ลาออก

(๓) คณะรัฐมนตรีให้ออก

(๔) ขาดคุณสมบัติหรือมีลักษณะต้องห้ามตามมาตรา ๖

มาตรา ๙ คณะกรรมการมีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมและสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๒ และมาตรา ๔๓ ต่อคณะรัฐมนตรีเพื่อให้ความเห็นชอบ ซึ่งต้องเป็นไปตามแนวทางที่กำหนดไว้ในมาตรา ๔๒

(๒) กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรี สำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติและกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาพความมั่นคงแห่งชาติ

(๔) กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และกำหนดมาตรฐานขั้นต่ำที่เกี่ยวข้องกับคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน

(๕) กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๖) กำหนดกรอบการประสานความร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๗) แต่งตั้งและถอดถอนเลขาธิการ

(๘) มอบหมายการควบคุมและกำกับดูแล รวมถึงการออกข้อกำหนด วัตถุประสงค์ หน้าที่และอำนาจ และกรอบการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๙) ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์และการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่บัญญัติไว้ในพระราชบัญญัตินี้

(๑๐) เสนอแนะและให้ความเห็นต่อคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติหรือคณะรัฐมนตรี เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๑) เสนอแนะต่อคณะรัฐมนตรีในการจัดให้มีหรือปรับปรุงกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๒) จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญหรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้คณะรัฐมนตรีทราบ

(๑๓) ปฏิบัติการอื่นใดตามที่บัญญัติไว้ในพระราชบัญญัตินี้ หรือคณะรัฐมนตรีมอบหมาย

มาตรา ๑๐ การประชุมของคณะกรรมการ ให้เป็นไปตามระเบียบที่คณะกรรมการกำหนด โดยอาจประชุมด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นก็ได้

มาตรา ๑๑ ให้ประธานกรรมการ และกรรมการได้รับเบี้ยประชุมหรือค่าตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

ส่วนที่ ๒

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

มาตรา ๑๒ ในการดำเนินการตามหน้าที่และอำนาจของคณะกรรมการตามมาตรา ๙ ให้มีคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กกม.” ประกอบด้วย

(๑) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานกรรมการ

(๒) กรรมการโดยตำแหน่ง ได้แก่ ปลัดกระทรวงการต่างประเทศ ปลัดกระทรวงคมนาคม ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ปลัดกระทรวงพลังงาน ปลัดกระทรวงมหาดไทย ปลัดกระทรวงสาธารณสุข ผู้บัญชาการตำรวจแห่งชาติ ผู้บัญชาการทหารสูงสุด เลขาธิการสภาความมั่นคงแห่งชาติ ผู้อำนวยการสำนักข่าวกรองแห่งชาติ ผู้ว่าการธนาคารแห่งประเทศไทย เลขาธิการสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และเลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

(๓) กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกินสี่คน ซึ่งคณะกรรมการแต่งตั้งจากผู้มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

หลักเกณฑ์และวิธีการสรรหาบุคคลที่เห็นสมควรเพื่อพิจารณาแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิให้เป็นไปตามระเบียบที่คณะกรรมการกำหนด

มาตรา ๑๓ กกม. มีหน้าที่และอำนาจ ดังต่อไปนี้

(๑) ติดตามการดำเนินการตามนโยบายและแผนตามมาตรา ๙ (๑) และมาตรา ๔๒

(๒) ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ตามมาตรา ๖๑ มาตรา ๖๒ มาตรา ๖๓ มาตรา ๖๔ มาตรา ๖๕ และมาตรา ๖๖

(๓) กำกับดูแลการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ และการเผชิญเหตุและนิติวิทยาศาสตร์ทางคอมพิวเตอร์

(๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

(๕) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือกำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ

(๖) กำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์ในแต่ละระดับเสนอต่อคณะกรรมการ

(๗) วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ เพื่อเสนอต่อคณะกรรมการพิจารณาสั่งการ เมื่อมีหรือคาดว่าจะมีภัยคุกคามทางไซเบอร์ในระดับร้ายแรงขึ้น

ในการกำหนดกรอบมาตรฐานตามวรรคหนึ่ง (๔) ให้คำนึงถึงหลักการบริหารความเสี่ยง โดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ ดังต่อไปนี้

(๑) การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๒) มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

มาตรา ๑๔ ในการดำเนินการตามมาตรา ๑๓ วรรคหนึ่ง (๒) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ได้ทันทั่วทั้งที่ กกม. อาจมอบอำนาจให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ผู้บัญชาการทหารสูงสุด และกรรมการอื่นซึ่ง กกม. กำหนด ร่วมกันปฏิบัติการในเรื่องดังกล่าวได้ และจะกำหนดให้หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่ถูกคุกคามเข้าร่วมดำเนินการ ประสานงาน และให้การสนับสนุนด้วยก็ได้

การปฏิบัติตามวรรคหนึ่ง ให้เป็นไปตามระเบียบที่ กกม. กำหนด

มาตรา ๑๕ ให้นำความในมาตรา ๖ มาตรา ๗ และมาตรา ๘ มาใช้บังคับกับกรรมการผู้ทรงคุณวุฒิใน กกม. โดยอนุโลม

มาตรา ๑๖ ให้ กกม. มีอำนาจแต่งตั้งคณะกรรมการเพื่อปฏิบัติการอย่างใดอย่างหนึ่งตามที่ กกม. มอบหมาย

มาตรา ๑๗ การประชุมของ กกม. และคณะกรรมการ ให้เป็นไปตามระเบียบที่ กกม. กำหนด โดยอาจประชุมด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นก็ได้

มาตรา ๑๘ ให้ประธานกรรมการและกรรมการ ประธานอนุกรรมการและอนุกรรมการที่ กกม. แต่งตั้ง ได้รับเบี้ยประชุมหรือค่าตอบแทนอื่นตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

มาตรา ๑๙ ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ พนักงานเจ้าหน้าที่ต้องแสดงบัตรประจำตัวต่อบุคคลที่เกี่ยวข้อง

ในการแต่งตั้งพนักงานเจ้าหน้าที่ ให้รัฐมนตรีพิจารณาแต่งตั้งจากผู้มีความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นพนักงานเจ้าหน้าที่เพื่อปฏิบัติการอย่างหนึ่งอย่างใดตามพระราชบัญญัตินี้ ทั้งนี้ ระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ ให้เป็นไปตามที่คณะกรรมการประกาศกำหนด

บัตรประจำตัวพนักงานเจ้าหน้าที่ให้เป็นไปตามแบบที่ กกม. ประกาศกำหนด

หมวด ๒

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๒๐ ให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น

มาตรา ๒๑ กิจการของสำนักงานไม่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยแรงงานสัมพันธ์ กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน แต่พนักงานและลูกจ้างของสำนักงานต้องได้รับประโยชน์ตอบแทนไม่น้อยกว่าที่กำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน

มาตรา ๒๒ ให้สำนักงานรับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของคณะกรรมการ และ กกม. และให้มีหน้าที่และอำนาจดังต่อไปนี้ด้วย

(๑) เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๙ ต่อคณะกรรมการ

(๒) จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) เสนอต่อ กกม. เพื่อให้ความเห็นชอบ

(๓) ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๕๓ และมาตรา ๕๔

(๔) ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์

(๕) ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจากคณะกรรมการ

(๖) เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(๗) ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์หรือตามคำสั่งของคณะกรรมการ

(๘) ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๙) เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้าง ความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการ ที่มีลักษณะบูรณาการและเป็นปัจจุบัน

(๑๐) เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน

(๑๑) เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคง ปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ

(๑๒) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการที่เกี่ยวข้องกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจากคณะกรรมการ

(๑๓) ศึกษาและวิจัยข้อมูลที่สำคัญสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ

(๑๔) ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

(๑๕) รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้งปัญหาและอุปสรรค เสนอต่อคณะกรรมการเพื่อพิจารณาดำเนินการ ทั้งนี้ ตามระยะเวลาที่คณะกรรมการกำหนด

(๑๖) ปฏิบัติงานอื่นใดอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามที่คณะกรรมการหรือคณะรัฐมนตรีมอบหมาย

เพื่อประโยชน์ในการดำเนินการตามหน้าที่และอำนาจตาม (๖) ให้สำนักงานจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติขึ้นเป็นหน่วยงานภายในสำนักงาน และให้มีหน้าที่และอำนาจตามที่คณะกรรมการกำหนด

มาตรา ๒๓ ในการดำเนินการของสำนักงาน นอกจากหน้าที่และอำนาจตามที่บัญญัติในมาตรา ๒๒ แล้ว ให้สำนักงานมีหน้าที่และอำนาจทั่วไปดังต่อไปนี้ด้วย

(๑) ถือกรรมสิทธิ์ มีสิทธิครอบครอง และมีทรัพย์สินต่าง ๆ

(๒) ก่อตั้งสิทธิ หรือทำนิติกรรมทุกประเภทผูกพันทรัพย์สิน ตลอดจนทำนิติกรรมอื่นใดเพื่อประโยชน์ในการดำเนินการของสำนักงาน

(๓) จัดให้มีและให้ทุนเพื่อสนับสนุนการดำเนินการของสำนักงาน

(๔) เรียกเก็บค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน หรือค่าบริการในการดำเนินงาน ทั้งนี้ ตามหลักเกณฑ์และอัตราที่สำนักงานกำหนดโดยความเห็นชอบของ กบส.

(๕) ปฏิบัติการอื่นใดที่กฎหมายกำหนดให้เป็นหน้าที่และอำนาจของสำนักงาน หรือตามที่คณะกรรมการ หรือ กบส. มอบหมาย

มาตรา ๒๔ ทุนและทรัพย์สินในการดำเนินงานของสำนักงาน ประกอบด้วย

(๑) ทุนประเดิมที่รัฐบาลจัดสรรให้ตามมาตรา ๘๑ วรรคหนึ่ง และเงินและทรัพย์สินที่ได้รับโอนตามมาตรา ๘๒

(๒) เงินอุดหนุนทั่วไปที่รัฐบาลจัดสรรให้ตามความเหมาะสมเป็นรายปี

(๓) เงินอุดหนุนจากหน่วยงานของรัฐทั้งในประเทศและต่างประเทศ หรือองค์การระหว่างประเทศ ระดับรัฐบาล

(๔) ค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน ค่าบริการ หรือรายได้อันเกิดจากการดำเนินการตามหน้าที่และอำนาจของสำนักงาน

(๕) ดอกผลของเงินหรือรายได้จากทรัพย์สินของสำนักงาน

เงินและทรัพย์สินของสำนักงานตามวรรคหนึ่ง ต้องนำส่งคลังเป็นรายได้แผ่นดิน

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

ให้เลขาธิการเป็นกรรมการและเลขานุการ และให้เลขาธิการแต่งตั้งพนักงานของสำนักงานเป็นผู้ช่วยเลขานุการได้ไม่เกินสองคน

กรรมการผู้ทรงคุณวุฒิตามวรรคหนึ่ง ให้รัฐมนตรีแต่งตั้งจากบุคคลซึ่งมีความรู้ ความเชี่ยวชาญ และความสามารถเป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศ และการสื่อสาร ด้านเศรษฐศาสตร์ ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านบริหารธุรกิจ หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการดำเนินงานของ กบส. ตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด

ให้นำความในมาตรา ๖ และมาตรา ๘ มาใช้บังคับกับกรรมการผู้ทรงคุณวุฒิโดยอนุโลม

มาตรา ๒๖ ให้กรรมการผู้ทรงคุณวุฒิใน กบส. มีวาระการดำรงตำแหน่งคราวละสี่ปี

ในกรณีที่มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งก่อนวาระ รัฐมนตรีอาจแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างได้ และให้ผู้ได้รับแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของกรรมการผู้ทรงคุณวุฒิซึ่งได้แต่งตั้งไว้แล้ว

เมื่อครบกำหนดวาระตามวรรคหนึ่ง หากยังมิได้แต่งตั้งกรรมการผู้ทรงคุณวุฒิชั้นใหม่ ให้กรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งตามวาระนั้นอยู่ในตำแหน่งเพื่อดำเนินงานต่อไปจนกว่าจะได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิชั้นใหม่

มาตรา ๒๗ ให้ กบส. มีหน้าที่และอำนาจ ดังต่อไปนี้

- (๑) กำหนดนโยบายการบริหารงาน และให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน
- (๒) ออกข้อบังคับว่าด้วยการจัดองค์กร การเงิน การบริหารงานบุคคล การบริหารงานทั่วไป การพัสดุ การตรวจสอบภายใน รวมตลอดทั้งการสงเคราะห์และสวัสดิการต่าง ๆ ของสำนักงาน
- (๓) อนุมัติแผนการใช้จ่ายเงินและงบประมาณรายจ่ายประจำปีของสำนักงาน
- (๔) ควบคุมการบริหารงานและการดำเนินการของสำนักงานและเลขาธิการ ให้เป็นไปตามพระราชบัญญัตินี้และกฎหมายอื่นที่เกี่ยวข้อง
- (๕) วินิจฉัยคำสั่งทางปกครองของเลขาธิการในส่วนที่เกี่ยวกับการบริหารงานของสำนักงาน
- (๖) ประเมินผลการดำเนินงานของสำนักงานและการปฏิบัติงานของเลขาธิการ
- (๗) ปฏิบัติหน้าที่อื่นตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นหน้าที่และอำนาจของ กบส. หรือตามที่คณะกรรมการหรือคณะรัฐมนตรีมอบหมาย

ในการปฏิบัติงานตามวรรคหนึ่ง กบส. อาจแต่งตั้งคณะกรรมการเพื่อพิจารณา เสนอแนะ หรือกระทำการอย่างหนึ่งอย่างใดตามที่ กบส. มอบหมายได้ ทั้งนี้ การปฏิบัติงานและการประชุม ให้เป็นไปตามหลักเกณฑ์และวิธีการที่ กบส. กำหนด

กบส. อาจแต่งตั้งผู้ทรงคุณวุฒิซึ่งมีความเชี่ยวชาญในด้านที่เป็นประโยชน์ต่อการดำเนินงานของสำนักงานเป็นที่ปรึกษา กบส. ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด

มาตรา ๒๘ ให้ประธานกรรมการและกรรมการ ประธานอนุกรรมการและอนุกรรมการ ที่ กบส. แต่งตั้ง ได้รับเบี้ยประชุมและค่าตอบแทนอื่นตามหลักเกณฑ์ที่คณะกรรมการกำหนด

มาตรา ๒๙ ให้สำนักงานมีเลขาธิการคนหนึ่ง รับผิดชอบการปฏิบัติงานของสำนักงาน และเป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน

มาตรา ๓๐ เลขาธิการต้องมีคุณสมบัติ ดังต่อไปนี้

- (๑) มีสัญชาติไทย
- (๒) มีอายุไม่ต่ำกว่าสามสิบห้าปี แต่ไม่เกินหกสิบปี
- (๓) เป็นผู้มีความรู้ ความสามารถ และประสบการณ์ในด้านที่เกี่ยวกับภารกิจของสำนักงาน และการบริหารจัดการ

มาตรา ๓๑ ผู้มีลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้ ต้องห้ามมิให้เป็นเลขาธิการ

- (๑) เป็นบุคคลล้มละลายหรือเคยเป็นบุคคลล้มละลายทุจริต
- (๒) เป็นคนไร้ความสามารถหรือคนเสมือนไร้ความสามารถ
- (๓) เคยต้องคำพิพากษาถึงที่สุดให้จำคุกไม่ว่าจะได้รับโทษจำคุกจริงหรือไม่ เว้นแต่เป็นโทษสำหรับความผิดที่ได้กระทำโดยประมาทหรือความผิดลหุโทษ
- (๔) เป็นข้าราชการ พนักงาน หรือลูกจ้าง ของส่วนราชการหรือรัฐวิสาหกิจหรือหน่วยงานอื่นของรัฐหรือของราชการส่วนท้องถิ่น
- (๕) เป็นหรือเคยเป็นข้าราชการการเมือง ผู้ดำรงตำแหน่งทางการเมือง สมาชิกสภาท้องถิ่นหรือผู้บริหารท้องถิ่น เว้นแต่จะพ้นจากตำแหน่งมาแล้วไม่น้อยกว่าหนึ่งปี
- (๖) เป็นหรือเคยเป็นกรรมการหรือผู้ดำรงตำแหน่งอื่นในพรรคการเมืองหรือเจ้าหน้าที่ของพรรคการเมือง เว้นแต่จะพ้นจากตำแหน่งมาแล้วไม่น้อยกว่าหนึ่งปี
- (๗) เคยถูกไล่ออก ปลดออก หรือให้ออกจากราชการ หรือออกจากงานจากหน่วยงานที่เคยปฏิบัติหน้าที่ เพราะทุจริตต่อหน้าที่หรือประพฤติชั่วอย่างร้ายแรง หรือเคยถูกถอดถอนจากตำแหน่ง
- (๘) เคยถูกให้ออกเพราะไม่ผ่านการประเมินผลการปฏิบัติงานตามมาตรา ๓๕ (๕)

มาตรา ๓๒ ให้คณะกรรมการเป็นผู้กำหนดอัตราเงินเดือนและค่าตอบแทนอื่นของเลขาธิการตามหลักเกณฑ์ที่คณะรัฐมนตรีกำหนด

มาตรา ๓๓ เลขาธิการมีวาระอยู่ในตำแหน่งคราวละสี่ปี

เลขาธิการซึ่งพ้นจากตำแหน่งตามวาระอาจได้รับแต่งตั้งอีกได้ แต่ต้องไม่เกินสองวาระ

มาตรา ๓๔ ในแต่ละปี ให้มีการประเมินผลการปฏิบัติงานของเลขาธิการ ทั้งนี้ ให้เป็นไปตามระยะเวลาและวิธีการที่คณะกรรมการกำหนด

มาตรา ๓๕ นอกจากการพ้นจากตำแหน่งตามวาระ เลขาธิการพ้นจากตำแหน่ง เมื่อ

- (๑) ตาย
- (๒) ลาออก
- (๓) ขาดคุณสมบัติตามมาตรา ๓๐ หรือมีลักษณะต้องห้ามตามมาตรา ๓๑
- (๔) คณะกรรมการมีมติให้ออก เพราะบกพร่องหรือทุจริตต่อหน้าที่ มีความประพฤติเสื่อมเสียหรือหย่อนความสามารถ
- (๕) คณะกรรมการให้ออก เพราะไม่ผ่านการประเมินผลการปฏิบัติงาน
- (๖) ออกตามกรณีที่กำหนดไว้ในสัญญาจ้างหรือข้อตกลงระหว่างคณะกรรมการกับเลขาธิการ

มาตรา ๓๖ ให้เลขาธิการภายใต้การควบคุมดูแลของคณะกรรมการ กกม. และ กบส. ต้องดำเนินการตามคำสั่งของคณะกรรมการ กกม. และ กบส. ภายใต้หน้าที่และอำนาจ ดังต่อไปนี้

(๑) บริหารงานของสำนักงานให้เกิดผลสัมฤทธิ์ตามภารกิจของสำนักงาน และตามนโยบาย และแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคง ปลอดภัยไซเบอร์ นโยบายของคณะรัฐมนตรีและคณะกรรมการ และข้อบังคับ นโยบาย มติ และ ประกาศของ กบส.

(๒) วางระเบียบภายใต้นโยบายของคณะกรรมการและ กกม. โดยไม่ขัดหรือแย้งกับกฎหมาย มติของคณะรัฐมนตรี และข้อบังคับ นโยบาย มติ และประกาศที่คณะกรรมการและ กกม. กำหนด

(๓) เป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน และประเมินผลการปฏิบัติงานของ พนักงานและลูกจ้างของสำนักงานตามข้อบังคับของ กบส. และระเบียบของสำนักงาน

(๔) แต่งตั้งรองเลขาธิการหรือผู้ช่วยเลขาธิการโดยความเห็นชอบของคณะกรรมการ เพื่อเป็น ผู้ช่วยปฏิบัติงานของเลขาธิการตามที่เลขาธิการมอบหมาย

(๕) บรรจุ แต่งตั้ง เลื่อน ลด ตัดเงินเดือนหรือค่าจ้าง ลงโทษทางวินัยพนักงานและลูกจ้าง ของสำนักงาน ตลอดจนให้พนักงานและลูกจ้างของสำนักงานออกจากตำแหน่ง ทั้งนี้ ตามข้อบังคับของ กบส. และระเบียบของสำนักงาน

(๖) ปฏิบัติการอื่นใดตามข้อบังคับ นโยบาย มติ หรือประกาศของ กบส. หรือ กกม.

ในกิจการของสำนักงานที่เกี่ยวกับบุคคลภายนอก ให้เลขาธิการเป็นผู้แทนของสำนักงาน ภายใต้ขอบเขตที่ได้รับการแต่งตั้งโดยคณะกรรมการ

เลขาธิการอาจมอบอำนาจให้บุคคลใดในสังกัดของสำนักงาน ปฏิบัติงานเฉพาะอย่างแทนก็ได้ ทั้งนี้ ตามข้อบังคับที่ กบส. กำหนด

ในกรณีที่ไม่มีเลขาธิการหรือเลขาธิการไม่อาจปฏิบัติหน้าที่ได้ ให้รองเลขาธิการที่มีอาวุโส ตามลำดับรักษาการแทน ถ้าไม่มีรองเลขาธิการหรือรองเลขาธิการไม่อาจปฏิบัติหน้าที่ได้ ให้คณะกรรมการ แต่งตั้งบุคคลที่เหมาะสมมารักษาการแทน

มาตรา ๓๗ การบัญชีของสำนักงานให้จัดทำตามแบบและหลักเกณฑ์ที่ กบส. กำหนด โดยให้คำนึงถึงหลักสากลและมาตรฐานการบัญชี

มาตรา ๓๘ ให้สำนักงานจัดทำงบการเงินและบัญชี แล้วส่งผู้สอบบัญชีภายในเก้าสิบวัน นับแต่วันสิ้นปีบัญชี

ให้สำนักงานการตรวจเงินแผ่นดินหรือผู้สอบบัญชีรับอนุญาตที่สำนักงานการตรวจเงินแผ่นดินให้ความเห็นชอบเป็นผู้สอบบัญชีของสำนักงาน และประเมินผลการใช้จ่ายเงินและทรัพย์สินของสำนักงานในรอบปีแล้วทำรายงานผลการสอบบัญชีเสนอต่อ กบส. เพื่อรับรอง

มาตรา ๓๙ ให้สำนักงานจัดทำรายงานผลการดำเนินงานประจำปีเสนอคณะกรรมการและรัฐมนตรีภายในหนึ่งร้อยแปดสิบวันนับแต่วันสิ้นปีบัญชี และเผยแพร่รายงานนี้ต่อสาธารณชน

รายงานผลการดำเนินงานประจำปีตามวรรคหนึ่ง ให้แสดงรายละเอียดของงบการเงินที่ผู้สอบบัญชีให้ความเห็นแล้ว พร้อมทั้งผลงานของสำนักงานและรายงานการประเมินผลการดำเนินงานของสำนักงานในปีที่ล่วงมาแล้ว

การประเมินผลการดำเนินงานของสำนักงานตามวรรคสอง จะต้องดำเนินการโดยบุคคลภายนอกที่ กบส. ให้ความเห็นชอบ

มาตรา ๔๐ ให้รัฐมนตรีมีอำนาจกำกับดูแลโดยทั่วไปซึ่งกิจการของสำนักงานให้เป็นไปตามหน้าที่และอำนาจของสำนักงาน กฎหมาย แผนยุทธศาสตร์ชาติ นโยบายและแผนของรัฐบาล และมติคณะรัฐมนตรีที่เกี่ยวข้อง เพื่อการนี้ให้รัฐมนตรีมีอำนาจสั่งให้เลขาธิการชี้แจงข้อเท็จจริง แสดงความคิดเห็น หรือทำรายงานเสนอ และมีอำนาจสั่งยับยั้งการกระทำของสำนักงานที่ขัดต่อหน้าที่และอำนาจของสำนักงาน กฎหมาย แผนยุทธศาสตร์ชาติ นโยบายและแผนของรัฐบาล หรือมติคณะรัฐมนตรีที่เกี่ยวข้อง ตลอดจนสั่งสอบสวนข้อเท็จจริงเกี่ยวกับการดำเนินการของสำนักงานได้

หมวด ๓

การรักษาความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑

นโยบายและแผน

มาตรา ๔๑ การรักษาความมั่นคงปลอดภัยไซเบอร์ต้องคำนึงถึงความเป็นเอกภาพและการบูรณาการในการดำเนินงานของหน่วยงานของรัฐและหน่วยงานเอกชน และต้องสอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมตามกฎหมายว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

การดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมุ่งหมายเพื่อสร้างศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะอย่างยิ่งในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

มาตรา ๔๒ นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีเป้าหมายและแนวทางอย่างน้อย ดังต่อไปนี้

- (๑) การบูรณาการการจัดการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ
- (๒) การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
- (๓) การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ
- (๔) การประสานความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์
- (๕) การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- (๖) การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐและเอกชน
- (๗) การสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- (๘) การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๔๓ ให้คณะกรรมการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ขึ้นตามแนวทางในมาตรา ๔๒ เพื่อเสนอคณะรัฐมนตรีให้ความเห็นชอบ โดยให้ประกาศในราชกิจจานุเบกษา และเมื่อได้ประกาศแล้ว ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามที่กำหนดไว้ในแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการให้เป็นไปตามนโยบายและแผนดังกล่าว

ในการจัดทำนโยบายและแผนตามวรรคหนึ่ง ให้สำนักงานจัดให้มีการรับฟังความเห็นหรือประชุมร่วมกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง อย่างน้อยต้องประกอบด้วยเรื่อง ดังต่อไปนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

เพื่อประโยชน์ในการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่ง ให้สำนักงานโดยความเห็นชอบของคณะกรรมการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานดังกล่าวยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐานให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ

ส่วนที่ ๒

การบริหารจัดการ

มาตรา ๔๕ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง (๔) ด้วย

ในกรณีที่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่อาจดำเนินการหรือปฏิบัติตามวรรคหนึ่งได้ สำนักงานอาจให้ความช่วยเหลือด้านบุคลากรหรือเทคโนโลยีแก่หน่วยงานนั้นตามที่ร้องขอได้

มาตรา ๔๖ เพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน

ในกรณีที่มีการเปลี่ยนแปลงเจ้าหน้าที่ตามวรรคหนึ่ง ให้หน่วยงานของรัฐ หน่วยงานควบคุม หรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แจ้งให้สำนักงานทราบโดยเร็ว

มาตรา ๔๗ ในกรณีที่มีการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ต้องอาศัยความรู้ ความเชี่ยวชาญ คณะกรรมการหรือ กกม. อาจมอบหมายให้เลขาธิการว่าจ้างผู้เชี่ยวชาญตามความเหมาะสมเฉพาะงานได้ ผู้เชี่ยวชาญตามวรรคหนึ่งต้องมีคุณสมบัติหรือประสบการณ์ที่เหมาะสมตามที่คณะกรรมการ ประกาศกำหนด

เลขาธิการต้องออกบัตรประจำตัวผู้เชี่ยวชาญให้แก่บุคคลที่ได้รับการแต่งตั้ง และในการปฏิบัติหน้าที่ บุคคลดังกล่าวต้องแสดงบัตรประจำตัวในฐานะผู้เชี่ยวชาญ และเมื่อพ้นจากหน้าที่แล้วจะต้องคืน บัตรประจำตัวแก่สำนักงานโดยเร็ว

ส่วนที่ ๓

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มาตรา ๔๘ โครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นกิจการที่มีความสำคัญต่อความมั่นคง ของรัฐ ความมั่นคงทางทหาร ความมั่นคงทางเศรษฐกิจ และความสงบเรียบร้อยภายในประเทศ และเป็นหน้าที่ของสำนักงานในการสนับสนุนและให้ความช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ

มาตรา ๔๙ ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะหน่วยงานที่มีการกิจหรือ ให้บริการในด้านดังต่อไปนี้ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- (๑) ด้านความมั่นคงของรัฐ
- (๒) ด้านบริการภาครัฐที่สำคัญ
- (๓) ด้านการเงินการธนาคาร
- (๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม
- (๕) ด้านการขนส่งและโลจิสติกส์
- (๖) ด้านพลังงานและสาธารณูปโภค
- (๗) ด้านสาธารณสุข
- (๘) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

การพิจารณาประกาศกำหนดภารกิจหรือบริการตามวรรคหนึ่ง ให้เป็นไปตามหลักเกณฑ์ที่คณะกรรมการกำหนด โดยประกาศในราชกิจจานุเบกษา ทั้งนี้ คณะกรรมการจะต้องพิจารณาทบทวนการประกาศกำหนดภารกิจหรือบริการดังกล่าวเป็นคราว ๆ ไปตามความเหมาะสม

มาตรา ๕๐ ให้คณะกรรมการมีอำนาจประกาศกำหนดลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ เพื่อประสานงาน ใ้ระวัง รับมือ และแก้ไขภัยคุกคามทางไซเบอร์ โดยจะกำหนดให้หน่วยงานของรัฐที่มีความพร้อมหรือหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ๆ ทำหน้าที่ดังกล่าวให้แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ทั้งหมดหรือบางส่วนก็ได้

การพิจารณาประกาศกำหนดภารกิจหรือบริการของหน่วยงานตามวรรคหนึ่ง ให้เป็นไปตามหลักเกณฑ์ที่คณะกรรมการกำหนด โดยประกาศในราชกิจจานุเบกษา ทั้งนี้ คณะกรรมการจะต้องพิจารณาทบทวนการประกาศกำหนดภารกิจหรือบริการดังกล่าวเป็นคราว ๆ ไปตามความเหมาะสม

มาตรา ๕๑ กรณีมีข้อสงสัยหรือข้อโต้แย้งเกี่ยวกับลักษณะหน่วยงานที่มีภารกิจหรือให้บริการในด้านที่มีการประกาศกำหนดตามมาตรา ๔๙ หรือมาตรา ๕๐ ให้คณะกรรมการเป็นผู้วินิจฉัยชี้ขาด

มาตรา ๕๒ เพื่อประโยชน์ในการติดต่อประสานงาน ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งรายชื่อและข้อมูลการติดต่อของเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ไปยังสำนักงาน หน่วยงานควบคุมหรือกำกับดูแลของตน และหน่วยงานตามมาตรา ๕๐ ภายในสามสิบวันนับแต่วันที่คณะกรรมการประกาศตามมาตรา ๔๙ วรรคสอง และมาตรา ๕๐ วรรคสอง หรือนับแต่วันที่คณะกรรมการมีคำวินิจฉัยตามมาตรา ๕๑ แล้วแต่กรณี โดยอย่างน้อยเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ต้องเป็นบุคคลซึ่งรับผิดชอบในการบริหารงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น

ในกรณีที่มีการเปลี่ยนแปลงเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ตามวรรคหนึ่ง ให้แจ้งการเปลี่ยนแปลงไปยังหน่วยงานที่เกี่ยวข้องตามวรรคหนึ่งก่อนการเปลี่ยนแปลงล่วงหน้าไม่น้อยกว่าเจ็ดวัน เว้นแต่มีเหตุจำเป็นอันไม่อาจก้วล้งได้ให้แจ้งโดยเร็ว

มาตรา ๕๓ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานควบคุมหรือกำกับดูแลตรวจสอบมาตรฐานขั้นต่ำเรื่องความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ภายใต้การกำกับควบคุมดูแลของตน หากพบว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่ได้มาตรฐาน ให้หน่วยงานควบคุม

หรือกำกับดูแลนั้นรับแจ้งให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ต่ำกว่ามาตรฐานแก้ไขให้ได้มาตรฐานโดยเร็ว หากหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นยังคงเพิกเฉยไม่ดำเนินการหรือไม่ดำเนินการให้แล้วเสร็จภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด ให้หน่วยงานควบคุมหรือกำกับดูแลส่งเรื่องให้ กกม. พิจารณาโดยไม่ชักช้า

เมื่อได้รับคำร้องเรียนตามวรรคหนึ่ง หาก กกม. พิจารณาแล้วเห็นว่า มีเหตุดังกล่าวและอาจทำให้เกิดภัยคุกคามทางไซเบอร์ ให้ กกม. ดำเนินการ ดังต่อไปนี้

(๑) กรณีเป็นหน่วยงานของรัฐ ให้แจ้งต่อผู้บริหารระดับสูงสุดของหน่วยงานเพื่อใช้อำนาจในทางบริหาร สั่งการไปยังหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นเพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว

(๒) กรณีเป็นหน่วยงานเอกชน ให้แจ้งไปยังผู้บริหารระดับสูงสุดของหน่วยงาน ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นเพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว

ให้เลขาธิการดำเนินการติดตามเพื่อให้เป็นไปตามความในวรรคสองด้วย

มาตรา ๕๔ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละหนึ่งครั้ง

ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ

มาตรา ๕๕ ในกรณีที่ กกม. เห็นว่า การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๕๔ ไม่เป็นไปตามมาตรฐานตามรายงานของหน่วยงานควบคุมหรือกำกับดูแล ให้ กกม. มีคำสั่งให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้นดำเนินการประเมินความเสี่ยงใหม่เพื่อให้เป็นไปตามมาตรฐานหรือดำเนินการตรวจสอบในด้านอื่น ๆ ที่มีผลต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้

ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น ได้จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์หรือการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ตามวรรคหนึ่งแล้ว แต่ กกม. เห็นว่ายังไม่เป็นไปตามมาตรฐาน ให้ กกม. ดำเนินการ ดังต่อไปนี้

(๑) กรณีเป็นหน่วยงานของรัฐ ให้แจ้งต่อผู้บริหารระดับสูงสุดของหน่วยงานเพื่อใช้อำนาจในทางบริหาร สั่งการไปยังหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว

(๒) กรณีเป็นหน่วยงานเอกชน ให้แจ้งไปยังผู้บริหารระดับสูงสุดของหน่วยงาน ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนั้น เพื่อให้ดำเนินการแก้ไขจนได้มาตรฐานโดยเร็ว

ให้เลขาธิการดำเนินการติดตามเพื่อให้เป็นไปตามความในวรรคสองด้วย

มาตรา ๕๖ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องกำหนดให้มีกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน ตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการหรือ กกม. กำหนด และต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น

มาตรา ๕๗ เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแล และปฏิบัติการรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดในส่วนที่ ๔ ทั้งนี้ กกม. อาจกำหนดหลักเกณฑ์และวิธีการการรายงานด้วยก็ได้

ส่วนที่ ๔

การรับมือกับภัยคุกคามทางไซเบอร์

มาตรา ๕๘ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

ในกรณีที่หน่วยงานหรือบุคคลใดพบอุปสรรคหรือปัญหาในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ของตน หน่วยงานหรือบุคคลนั้นอาจร้องขอความช่วยเหลือไปยังสำนักงาน

มาตรา ๕๙ เมื่อปรากฏแก่หน่วยงานควบคุมหรือกำกับดูแล หรือเมื่อหน่วยงานควบคุมหรือกำกับดูแลได้รับแจ้งเหตุตามมาตรา ๕๘ ให้หน่วยงานควบคุมหรือกำกับดูแล ร่วมกับหน่วยงานตามมาตรา ๕๐ รวบรวมข้อมูล ตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และดำเนินการ ดังต่อไปนี้

(๑) สนับสนุนและให้ความช่วยเหลือแก่หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน และให้ความร่วมมือและประสานงานกับสำนักงาน ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(๒) แจ้งเตือนหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่อยู่ในการควบคุมหรือกำกับดูแลของตน รวมทั้งหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอื่นที่เกี่ยวข้องโดยเร็ว

มาตรา ๖๐ การพิจารณาเพื่อใช้อำนาจในการป้องกันภัยคุกคามทางไซเบอร์ คณะกรรมการจะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ ดังต่อไปนี้

(๑) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

(๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมีมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

(๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะ ดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรง

ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชนหรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องกันหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

ทั้งนี้ รายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ ให้คณะกรรมการเป็นผู้ประกาศกำหนด

มาตรา ๖๑ เมื่อปรากฏแก่ กกม. ว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรงให้ กกม. ออกคำสั่งให้สำนักงานดำเนินการ ดังต่อไปนี้

(๑) รวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้องเพื่อวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์

(๒) สนับสนุน ให้ความช่วยเหลือ และเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๓) ดำเนินการป้องกันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดจากภัยคุกคามทางไซเบอร์ เสนอแนะหรือสั่งการให้ใช้ระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการหาแนวทางตอบโต้หรือการแก้ไขปัญหาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๔) สนับสนุน ให้สำนักงาน และหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน ให้ความช่วยเหลือ และเข้าร่วมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๕) แจ้งเตือนภัยคุกคามทางไซเบอร์ให้ทราบโดยทั่วกัน ทั้งนี้ ตามความจำเป็นและเหมาะสม โดยคำนึงถึงสถานการณ์ ความร้ายแรงและผลกระทบจากภัยคุกคามทางไซเบอร์นั้น

(๖) ให้ความสะดวกในการประสานงานระหว่างหน่วยงานของรัฐที่เกี่ยวข้องและหน่วยงานเอกชน เพื่อจัดการความเสี่ยงและเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

มาตรา ๖๒ ในการดำเนินการตามมาตรา ๖๑ เพื่อประโยชน์ในการวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการสั่งให้พนักงานเจ้าหน้าที่ดำเนินการ ดังต่อไปนี้

(๑) มีหนังสือขอความร่วมมือจากบุคคลที่เกี่ยวข้องเพื่อมาให้ข้อมูลภายในระยะเวลาที่เหมาะสม และตามสถานที่ที่กำหนด หรือให้ข้อมูลเป็นหนังสือเกี่ยวกับภัยคุกคามทางไซเบอร์

(๒) มีหนังสือขอข้อมูล เอกสาร หรือสำเนาข้อมูลหรือเอกสารซึ่งอยู่ในความครอบครองของผู้อื่นอันเป็นประโยชน์แก่การดำเนินการ

(๓) สอบถามบุคคลผู้มีความรู้ความเข้าใจเกี่ยวกับข้อเท็จจริงและสถานการณ์ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์

(๔) เข้าไปในอสังหาริมทรัพย์หรือสถานประกอบการที่เกี่ยวข้องหรือคาดว่าจะมีส่วนเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ของบุคคลหรือหน่วยงานที่เกี่ยวข้อง โดยได้รับความยินยอมจากผู้ครอบครองสถานที่นั้น

ผู้ให้ข้อมูลตามวรรคหนึ่ง ซึ่งกระทำโดยสุจริตย่อมได้รับการคุ้มครองและไม่ถือว่าเป็นการละเมิดหรือผิดสัญญา

มาตรา ๖๓ ในกรณีที่มีความจำเป็นเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้ กกม. มีคำสั่งให้หน่วยงานของรัฐให้ข้อมูล สนับสนุนบุคลากรในสังกัด หรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

กกม. ต้องดูแลมิให้มีการใช้ข้อมูลที่ได้มาตามวรรคหนึ่งในลักษณะที่อาจก่อให้เกิดความเสียหาย และให้ กกม. รับผิดชอบในค่าตอบแทนบุคลากร ค่าใช้จ่ายหรือความเสียหายที่เกิดขึ้นจากการใช้เครื่องมือทางอิเล็กทรอนิกส์ดังกล่าว

ให้นำความในวรรคหนึ่งและวรรคสองมาใช้บังคับในการร้องขอต่อเอกชนโดยความยินยอมของเอกชนนั้นด้วย

มาตรา ๖๔ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง ให้ กกม. ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และดำเนินมาตรการที่จำเป็น

ในการดำเนินการตามวรรคหนึ่ง ให้ กกม. มีหนังสือถึงหน่วยงานของรัฐที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กระทำการหรือระงับการดำเนินการใด ๆ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสมและมีประสิทธิภาพตามแนวทางที่ กกม. กำหนด รวมทั้งร่วมกันบูรณาการในการดำเนินการเพื่อควบคุม ระงับ หรือบรรเทาผลที่เกิดจากภัยคุกคามทางไซเบอร์นั้นได้อย่างทันทั่วทั้งที่

ให้เลขาธิการรายงานการดำเนินการตามมาตรานี้ต่อ กกม. อย่างต่อเนื่อง และเมื่อภัยคุกคามทางไซเบอร์ดังกล่าวสิ้นสุดลง ให้รายงานผลการดำเนินการต่อ กกม. โดยเร็ว

มาตรา ๖๕ ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ให้บุคคลผู้เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ ซึ่งมีเหตุอันเชื่อได้ว่าเป็นผู้เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ดำเนินการ ดังต่อไปนี้

- (๑) ฝักระวังคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในช่วงระยะเวลาใดระยะเวลาหนึ่ง
- (๒) ตรวจสอบคอมพิวเตอร์หรือระบบคอมพิวเตอร์เพื่อหาข้อบกพร่องที่กระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์
- (๓) ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์เพื่อจัดการข้อบกพร่องหรือกำจัดชุดคำสั่งไม่พึงประสงค์ หรือระงับบรรเทาภัยคุกคามทางไซเบอร์ที่ดำเนินการอยู่
- (๔) รักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วยวิธีการใด ๆ เพื่อดำเนินการทางนิติวิทยาศาสตร์ทางคอมพิวเตอร์
- (๕) เข้าถึงข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ที่เกี่ยวข้องเฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์

ในกรณีมีเหตุจำเป็นที่ต้องเข้าถึงข้อมูลตาม (๕) ให้ กกม. มอบหมายให้เลขาธิการยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้เจ้าของกรรมสิทธิ์ ผู้ครอบครอง ผู้ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือผู้ดูแลระบบคอมพิวเตอร์ตามวรรคหนึ่งดำเนินการตามคำร้อง ทั้งนี้ คำร้องที่ยื่นต่อศาลต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดบุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

มาตรา ๖๖ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจปฏิบัติการหรือสั่งให้พนักงานเจ้าหน้าที่ปฏิบัติการเฉพาะเท่าที่จำเป็นเพื่อป้องกันภัยคุกคามทางไซเบอร์ในเรื่อง ดังต่อไปนี้

(๑) เข้าตรวจสอบสถานที่ โดยมีหนังสือแจ้งถึงเหตุอันสมควรไปยังเจ้าของหรือผู้ครอบครองสถานที่เพื่อเข้าตรวจสอบสถานที่นั้น หากมีเหตุอันควรเชื่อได้ว่ามีคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ หรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(๒) เข้าถึงข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทำสำเนา หรือสกัดคัดกรองข้อมูลสารสนเทศหรือโปรแกรมคอมพิวเตอร์ ซึ่งมีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

(๓) ทดสอบการทำงานของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าเกี่ยวข้องหรือได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ หรือถูกใช้เพื่อค้นหาข้อมูลใด ๆ ที่อยู่ภายในหรือใช้ประโยชน์จากคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น

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

ในการดำเนินการตาม (๒) (๓) และ (๔) ให้ กกม. ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใด บุคคลหนึ่งกำลังกระทำหรือจะกระทำการอย่างใดอย่างหนึ่งที่จะก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ในการพิจารณาคำร้องให้ยื่นเป็นคำร้องไต่สวนคำร้องฉุกเฉินและให้ศาลพิจารณาไต่สวนโดยเร็ว

มาตรา ๖๗ ในกรณีที่เกิดภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ให้เป็นหน้าที่และอำนาจของสภาความมั่นคงแห่งชาติ ในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกฎหมายว่าด้วยสภาความมั่นคงแห่งชาติและกฎหมายอื่นที่เกี่ยวข้อง

มาตรา ๖๘ ในกรณีที่เป็นเหตุจำเป็นเร่งด่วน และเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤติ คณะกรรมการอาจมอบหมายให้เลขาธิการมีอำนาจดำเนินการได้ทันทีเท่าที่จำเป็นเพื่อป้องกันและเยียวยาความเสียหายก่อนล่วงหน้าได้โดยไม่ต้องยื่นคำร้องต่อศาล แต่หลังจากการดำเนินการดังกล่าว ให้แจ้งรายละเอียดการดำเนินการดังกล่าวต่อศาลที่มีเขตอำนาจทราบโดยเร็ว

ในกรณีร้ายแรงหรือวิกฤติเพื่อประโยชน์ในการป้องกัน ประเมินผล รับมือ, ปราบปราม ระวัง และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้เลขาธิการโดยความเห็นชอบของคณะกรรมการหรือ กกม. มีอำนาจขอข้อมูลที่เป็นปัจจุบันและต่อเนื่องจากผู้ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ โดยผู้นั้น ต้องให้ความร่วมมือและให้ความสะดวกแก่คณะกรรมการหรือ กกม. โดยเร็ว

มาตรา ๖๙ ผู้ที่ได้รับคำสั่งอันเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์อาจอุทธรณ์คำสั่ง ได้เฉพาะที่เป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงเท่านั้น

หมวด ๔

บทกำหนดโทษ

มาตรา ๗๐ ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูล คอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูล ของผู้ใช้บริการ ที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิด ตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นหรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงาน เจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ

มาตรา ๗๑ พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่น ล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการหรือข้อมูลอื่นที่เกี่ยวข้องกับ ระบบคอมพิวเตอร์ ที่ได้มาตามพระราชบัญญัตินี้ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกิน สองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗๒ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ และ เปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗๓ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดไม่รายงานเหตุภัยคุกคาม ทางไซเบอร์ตามมาตรา ๕๗ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสองแสนบาท

มาตรา ๗๔ ผู้ใดไม่ปฏิบัติตามหนังสือเรียกของพนักงานเจ้าหน้าที่หรือไม่ส่งข้อมูลให้แก่พนักงานเจ้าหน้าที่ตามมาตรา ๖๒ (๑) หรือ (๒) โดยไม่มีเหตุอันสมควรแล้วแต่กรณี ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๗๕ ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กกม. ตามมาตรา ๖๕ (๑) และ (๒) โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกินสามแสนบาท และปรับอีกไม่เกินวันละหนึ่งหมื่นบาท นับแต่วันที่ครบกำหนดระยะเวลาที่ กกม. ออกคำสั่งให้ปฏิบัติจนกว่าจะปฏิบัติให้ถูกต้อง

ผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตามคำสั่งของ กกม. ตามมาตรา ๖๕ (๓) และ (๔) หรือไม่ปฏิบัติตามคำสั่งศาลตามมาตรา ๖๕ (๕) ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

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

มาตรา ๗๗ ในกรณีที่ผู้กระทำความผิดตามพระราชบัญญัตินี้เป็นนิติบุคคล ถ้าการกระทำความผิดของนิติบุคคลนั้นเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย

บทเฉพาะกาล

มาตรา ๗๘ ในวาระเริ่มแรก ให้คณะกรรมการประกอบด้วยประธานกรรมการและกรรมการตามมาตรา ๕ (๑) (๒) และให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นกรรมการและเลขานุการ เพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อน และให้ดำเนินการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของคณะกรรมการตามมาตรา ๕ (๓) ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

ในการแต่งตั้งกรรมการผู้ทรงคุณวุฒิตามวรรคหนึ่ง รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอาจเสนอรายชื่อบุคคลต่อคณะรัฐมนตรีเพื่อพิจารณาแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิดังกล่าวด้วยได้

มาตรา ๗๙ ให้ดำเนินการเพื่อให้มี กกม. และ กบส. ภายในเก้าสิบวันนับแต่วันที่ได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของคณะกรรมการตามมาตรา ๗๘

ให้ดำเนินการแต่งตั้งเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตามพระราชบัญญัตินี้ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่จัดตั้งสำนักงานแล้วเสร็จตามมาตรา ๘๐

มาตรา ๘๐ ให้ดำเนินการจัดตั้งสำนักงานให้แล้วเสร็จเพื่อปฏิบัติงานตามพระราชบัญญัตินี้ ภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

ในระหว่างที่การดำเนินการจัดตั้งสำนักงานยังไม่แล้วเสร็จ ให้สำนักงานปลัดกระทรวง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่สำนักงานตามพระราชบัญญัตินี้ และให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่เลขาธิการจนกว่าจะมีการแต่งตั้งเลขาธิการตามมาตรา ๗๙ วรรคสอง

มาตรา ๘๑ ในวาระเริ่มแรก ให้คณะรัฐมนตรีจัดสรรทุนประเดิมให้แก่สำนักงาน ตามความจำเป็น

ให้รัฐมนตรีเสนอต่อคณะรัฐมนตรีเพื่อพิจารณาให้ข้าราชการ พนักงาน เจ้าหน้าที่ หรือ ผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐ มาปฏิบัติงานที่สำนักงานเป็นการชั่วคราวภายในระยะเวลาที่ คณะรัฐมนตรีกำหนด

ให้ถือว่าข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐที่มาปฏิบัติงาน ในสำนักงานเป็นการชั่วคราวตามวรรคสองไม่ขาดจากสถานภาพเดิมและคงได้รับเงินเดือนหรือค่าจ้าง แล้วแต่กรณี จากสังกัดเดิม ทั้งนี้ คณะกรรมการอาจกำหนดค่าตอบแทนพิเศษให้แก่ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐตามวรรคสอง ในระหว่างปฏิบัติงานในสำนักงานด้วย ก็ได้

ภายในหนึ่งร้อยแปดสิบวันนับแต่วันที่จัดตั้งสำนักงานแล้วเสร็จ ให้สำนักงานดำเนินการคัดเลือก ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐตามวรรคสองเพื่อบรรจุ เป็นพนักงานของสำนักงานต่อไป

ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐผู้ใดได้รับการคัดเลือก และบรรจุตามวรรคสี่ ให้มีสิทธินับระยะเวลาทำงานที่เคยทำงานอยู่ในสังกัดเดิมต่อเนื่องรวมกับระยะเวลา ทำงานในสำนักงานตามพระราชบัญญัตินี้

มาตรา ๘๒ เมื่อพระราชบัญญัตินี้ใช้บังคับ ให้รัฐมนตรีเสนอคณะรัฐมนตรีดำเนินการเพื่ออนุมัติให้มีการโอนบรรดาอำนาจหน้าที่ กิจการ ทรัพย์สิน สิทธิ หนี้ และงบประมาณของบรรดาภารกิจที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานปลัดกระทรวง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ที่มีอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ไปเป็นของสำนักงานตามพระราชบัญญัตินี้

มาตรา ๘๓ การดำเนินการออกกฎกระทรวง ระเบียบ และประกาศ ตามพระราชบัญญัตินี้ ให้ดำเนินการให้แล้วเสร็จภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ ให้รัฐมนตรีรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

ผู้รับสนองพระบรมราชโองการ

พลเอก ประยุทธ์ จันทร์โอชา

นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่ในปัจจุบันการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียมมีความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ดังนั้น เพื่อให้สามารถป้องกัน หรือรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที สมควรกำหนดลักษณะของภารกิจหรือบริการที่มีความสำคัญเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งหน่วยงานของรัฐและหน่วยงานเอกชน ที่จะต้องมีการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ รวมทั้งให้มีหน่วยงานเพื่อรับผิดชอบในการดำเนินการประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนกำหนดให้มีแผนปฏิบัติการและมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างมีเอกภาพ และต่อเนื่อง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นต้องตราพระราชบัญญัตินี้

มติการประชุมคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

ครั้งที่ ๑/๒๕๖๓ วันอังคารที่ ๘ กันยายน ๒๕๖๓ เวลา ๑๓.๓๐ น.

ณ ห้องประชุม Think Big ชั้น ๒๐ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อาคารเดอะ โนน ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)

ระเบียบวาระ	มติที่ประชุม
ระเบียบวาระเพื่อพิจารณา ที่ ๓.๓ (ร่าง) คำขอจัดกลุ่มองค์การมหาชนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ฝ่ายเลขานุการฯ ได้รายงานต่อที่ประชุมว่าตามมาตรา ๒๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น โดยสำนักงานฯ ซึ่งถือเป็นองค์การมหาชนที่จัดตั้งตามพระราชบัญญัติเฉพาะตามหลักการจำแนกประเภทหน่วยงานของรัฐในกำกับของฝ่ายบริหาร ซึ่งต้องปฏิบัติหน้าที่สำคัญด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ เพื่อการพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามทางไซเบอร์ที่กระทบต่อความมั่นคงและเศรษฐกิจของชาติ หนังสือ สำนักงาน ก.พ.ร. ที่ นร ๑๒๐๘/๖๗๗ ลงวันที่ ๖ กันยายน ๒๕๖๒ เรื่อง แนวทางการดำเนินการตามมติคณะรัฐมนตรีของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดย สำนักงาน ก.พ.ร. ได้แจ้งให้ทราบ ดังนี้ - มติคณะรัฐมนตรีเมื่อวันที่ ๒๖ มีนาคม ๒๕๖๒ เห็นชอบให้คณะกรรมการพัฒนาและส่งเสริมองค์การมหาชน (กพม.) เป็นผู้พิจารณาเสนอความเห็นต่อคณะรัฐมนตรีในการจำแนกประเภทของหน่วยงานของรัฐที่จัดตั้งขึ้นใหม่แล้วแจ้งให้หน่วยงานที่เกี่ยวข้องทราบ - กพม. ในการประชุมครั้งที่ ๒/๒๕๖๒ เมื่อวันที่ ๑๖ สิงหาคม ๒๕๖๒ ได้พิจารณาและมีมติให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นองค์การมหาชนที่จัดตั้งตามพระราชบัญญัติเฉพาะตามมติคณะรัฐมนตรีเมื่อวันที่ ๒๐ ตุลาคม ๒๕๕๒ โดยแจ้งให้สำนักงานฯ ปฏิบัติตามมติคณะรัฐมนตรี โดยได้กำหนดให้ ส่งคำขอจัดกลุ่มองค์การมหาชนพร้อมข้อมูลประกอบการพิจารณา ได้แก่ วัตถุประสงค์ บทบาทภารกิจ องค์ประกอบคณะกรรมการบริหาร โครงสร้าง อัตรากำลัง ความยากง่ายหรือความยุ่งยากซับซ้อนของภารกิจ และสมรรถนะของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ไปยังสำนักงาน ก.พ.ร. เพื่อขอจัดกลุ่ม ในระหว่างที่ยังมิได้รับการจัดกลุ่มให้สำนักงานฯ เป็นองค์การมหาชนกลุ่ม ๓ (บริการสาธารณะทั่วไป) ไปพลางก่อน	เห็นชอบในหลักการ (ร่าง) คำขอจัดกลุ่มองค์การมหาชนของสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมอบหมายให้ฝ่ายเลขานุการฯ นำข้อสังเกตและข้อเสนอแนะจากที่ประชุมฯ ปรับแก้ไข (ร่าง) คำขอจัดกลุ่มองค์การมหาชนฯ ให้มีความสมบูรณ์ และดำเนินการในส่วนที่เกี่ยวข้องต่อไป

ระเบียบวาระ	มติที่ประชุม
- มติคณะรัฐมนตรีเมื่อวันที่ ๗ กันยายน ๒๕๔๗ เรื่อง หลักเกณฑ์การกำหนดอัตราเงินเดือนและประโยชน์ตอบแทนอื่นของผู้ดำรงการองค์การมหาชน (ผู้บริหารสูงสุดซึ่งเรียกชื่ออย่างอื่น) และหลักเกณฑ์การกำหนดเบี้ยประชุมและประโยชน์ตอบแทนอื่นของประธานกรรมการ กรรมการ (ใช้กับคณะกรรมการที่มีหน้าที่และอำนาจในการบริการและควบคุมดูแลการดำเนินงานขององค์การมหาชน ในกรณีนี้ คือ กบส.) ที่ปรึกษา และอนุกรรมการองค์การมหาชน ซึ่งจำแนกองค์การมหาชนเป็นสามกลุ่มตามมิติด้านความรับผิดชอบในการบริหารงาน มิติด้านประสบการณ์ของผู้ดำรงการ และมิติสถานการณ์ ทั้งนี้ มติคณะรัฐมนตรีเมื่อวันที่ ๒๖ มีนาคม ๒๕๖๒ กำหนดให้องค์การมหาชนที่จัดตั้งตามพระราชบัญญัติเฉพาะที่ยังมิได้รับการพิจารณาประเมินค่างานอยู่ในองค์การมหาชนกลุ่มที่ ๓ (บริการสาธารณะทั่วไป) ไปพลางก่อน หากองค์การมหาชนใด เห็นว่าภารกิจของหน่วยงานเป็นภารกิจตามลักษณะขององค์การมหาชนในกลุ่มที่ ๒ หรือ ๑ ให้ส่งคำขอมายังสำนักงาน ก.พ.ร. เพื่อเสนอ กพม. และคณะรัฐมนตรีพิจารณาต่อไป สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ทำหน้าที่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พิจารณาแล้ว เห็นว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีภารกิจตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนด ซึ่งเป็นองค์การมหาชนที่จัดตั้งขึ้นเพื่อพัฒนาและดำเนินการตามนโยบายสำคัญเฉพาะด้านของรัฐให้เกิดผลในทางปฏิบัติภายใต้ระยะเวลาจำกัด ซึ่งต้องการผู้บริหารที่มีความสามารถสูงในการบริหารงานเชิงยุทธศาสตร์ การบริหารเครือข่าย ทั้งในระดับประเทศและระหว่างประเทศ ซึ่งภารกิจของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ นั้นเข้าข่ายที่เป็นภารกิจตามลักษณะขององค์การมหาชนในกลุ่มที่ ๑ ฝ่ายเลขานุการ ได้จัดทำ (ร่าง) คำขอจัดกลุ่มองค์การมหาชนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรียบร้อยแล้ว โดยมีรายละเอียดข้อมูลประกอบการพิจารณา ได้แก่ วัตถุประสงค์ บทบาท ภารกิจ องค์ประกอบคณะกรรมการบริหาร โครงสร้าง อัตราค่าจ้าง ความยากง่ายหรือความยุ่งยากซับซ้อนของภารกิจ และสมรรถนะของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการนี้ จึงขอเสนอต่อที่ประชุมฯ เพื่อพิจารณาให้ความเห็นชอบต่อ (ร่าง) คำขอจัดกลุ่มองค์การมหาชนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และมอบหมายให้ฝ่ายเลขานุการฯ จัดส่งคำขอจัดกลุ่มองค์การมหาชนฯ ไปยังสำนักงาน ก.พ.ร. เพื่อเสนอ กพม. และคณะรัฐมนตรี ต่อไป	

**ข้อมูลประกอบการพิจารณา คำขอการจัดกลุ่มองค์การมหาชน
ในกลุ่มที่ 1 “พัฒนาและดำเนินการตามนโยบายสำคัญของรัฐเฉพาะด้าน”
ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ**

.....

ด้วยยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561-2580) ได้กำหนดให้ภัยไซเบอร์เป็นภัยที่มีผลกระทบต่อความมั่นคง โดยมีแผนย่อยของแผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง ซึ่งกำหนดแนวทางในการป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ มุ่งเน้นการวางกลยุทธ์/ยุทธวิธีในการแก้ไขปัญหา ด้านความมั่นคงทางไซเบอร์ ให้ครอบคลุมสภาพปัญหาของภัยคุกคามทางไซเบอร์ ได้แก่ การโจมตีทางไซเบอร์ของกลุ่มแฮกเกอร์ การจารกรรมหรือเปลี่ยนแปลงแก้ไขข้อมูล การโจมตีต่อกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการเผยแพร่ข้อมูลเพื่อความปั่นป่วนอันกระทบต่อประชาชนรวมทั้งอาจส่งผลกระทบต่อความมั่นคง โดยมีแนวคิดในการดำเนินการแก้ไขปัญหาที่สำคัญประการหนึ่ง คือ การจัดองค์กร โครงสร้าง อำนาจหน้าที่ ชัดความสามารถในการป้องกันและแก้ไขภัยความมั่นคงทางไซเบอร์

ทั้งนี้ ตามมาตรา 20 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจ ตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น โดยสำนักงานฯ ซึ่งถือเป็นองค์การมหาชนที่จัดตั้งตามพระราชบัญญัติเฉพาะตามหลักการจำแนกประเภทหน่วยงานของรัฐในกำกับของฝ่ายบริหาร ซึ่งต้องปฏิบัติหน้าที่สำคัญด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ เพื่อการพัฒนาศักยภาพของประเทศให้พร้อมเผชิญภัยคุกคามทางไซเบอร์ที่กระทบต่อความมั่นคงและเศรษฐกิจของชาติ ด้วยเหตุนี้ สำนักงานฯ จึงต้องมีแผนรองรับกับสภาวะภัยคุกคามทางไซเบอร์ของประเทศ มีความสามารถในการวิเคราะห์ รับมือ และป้องกันสถานการณ์ภัยคุกคามทางไซเบอร์ในทุกมิติอย่างทันทั่วทั้งที่สอดคล้องตามมาตรฐานสากล เพื่อให้สามารถปฏิบัติการกิจบรรลุตามวัตถุประสงค์ได้อย่างมีประสิทธิภาพ โดยเป็นที่ยอมรับทั้งในประเทศและระดับนานาชาติ

ในการนี้ สำนักงานฯ จึงต้องเป็นองค์กรที่มีสมรรถนะสูง เพื่อทำหน้าที่ในการประสานงานและบูรณาการความร่วมมือระหว่างภาครัฐและเอกชน อย่างเป็นรูปธรรม เพิ่มบทบาทการให้ข้อเสนอแนะเชิงนโยบายแก่รัฐบาล การดำเนินงานตอบสนองยุทธศาสตร์ชาติ ร่วมมือกับทุกภาคส่วนในการแก้ไขปัญหา สร้างนวัตกรรม แนวคิดใหม่ในการแก้ปัญหา และสร้างภูมิคุ้มกันเพื่อการพัฒนาประเทศอย่างยั่งยืน รวมทั้งเพื่อการขับเคลื่อนพันธกิจของรัฐบาลในการป้องกันและแก้ไขภัยคุกคามทางไซเบอร์ของประเทศให้สำเร็จโดยมุ่งยึดแนวทางการบริหารจัดการองค์กรอย่างมีธรรมาภิบาล และกลไกการกำกับตามที่ได้ออกแบบและระบุไว้ในพระราชบัญญัติฯ เป็นหลักก่อให้เกิดความไว้วางใจเป็นที่พึงของประชาชนทุกภาคส่วนอย่างแท้จริง

ดังนั้น สำนักงานฯ จึงจำเป็นต้องมีความคล่องตัวในการบริหารจัดการ มีประสิทธิภาพ โปร่งใส โดยบุคลากรที่ปฏิบัติงานด้านเทคนิคต้องมีความรู้ ความสามารถเฉพาะด้านความมั่นคงปลอดภัยไซเบอร์เป็นการเฉพาะ ประกอบกับบุคลากรในสาขานี้มีความขาดแคลน และที่ผ่านมาบุคลากรส่วนใหญ่จะทำงานในภาคเอกชน ซึ่งได้รับค่าตอบแทนที่สูงกว่าภาครัฐ ดังนั้นสำนักงานฯ จึงจำเป็นต้องมีระบบค่าตอบแทนที่เหมาะสมกับความสามารถของบุคลากร เพื่อสร้างแรงจูงใจและสรรหาบุคลากรเข้าสู่ตำแหน่งตามความเหมาะสม

ในการนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงขอเสนอการเป็นองค์การมหาชนในกลุ่มที่ 1 “พัฒนาและดำเนินการตามนโยบายสำคัญของรัฐเฉพาะด้าน”

1. วัตถุประสงค์

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อดำเนินงานตามนโยบายที่สำคัญเฉพาะด้านของรัฐบาล ในการรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ โดยกำหนดมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดการกระทำหรือการดำเนินการใด ๆ โดยมีขอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ มุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายอาจก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

2. บทบาทภารกิจ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีบทบาทภารกิจสำคัญตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ในมาตรา 22 ที่กำหนดให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติรับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรียกโดยย่อว่า “กมช.” และ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กกม.” และให้มีหน้าที่และอำนาจดังต่อไปนี้ด้วย

- (1) เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา 9 ต่อกมช.
- (2) จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา 13 วรรคหนึ่ง (4) เสนอต่อ กกม. เพื่อให้ความเห็นชอบ
- (3) ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา 53 และมาตรา 54
- (4) ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์
- (5) ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตามที่ได้รับมอบหมายจาก กมช.
- (6) เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์
- (7) ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ หรือตามคำสั่งของ กมช.
- (8) ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- (9) เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้าง ความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการ เชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน
- (10) เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน
- (11) เป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัย ไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ
- (12) ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและต่างประเทศในกิจการ ที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจาก กมช.
- (13) ศึกษาและวิจัยข้อมูลที่เป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะ เกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและ ฝึกซ้อม การรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ
- (14) ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัย ไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับ การรักษาความมั่นคงปลอดภัยไซเบอร์
- (15) รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้ง ปัญหาและ อุปสรรค เสนอต่อ กมช. เพื่อพิจารณาดำเนินการ ทั้งนี้ ตามระยะเวลาที่ กมช. กำหนด
- (16) ปฏิบัติงานอื่นใดอันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามที่ กมช. หรือ คณะรัฐมนตรีมอบหมาย

เพื่อประโยชน์ในการดำเนินการตามหน้าที่และอำนาจตาม (6) ให้สำนักงานจัดตั้งศูนย์ประสานการรักษา ความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติขึ้นเป็นหน่วยงานภายในสำนักงาน และให้มีหน้าที่และอำนาจ ตามที่ กมช. กำหนด

อีกทั้ง ตามมาตรา 23 แห่งพระราชบัญญัติฯ ได้กำหนดให้ ให้สำนักงานมีหน้าที่และอำนาจทั่วไป ดังต่อไปนี้ด้วย

- (1) ถือกรรมสิทธิ์ มีสิทธิครอบครอง และมีทรัพย์สินต่าง ๆ
- (2) ก่อตั้งสิทธิ หรือทำนิติกรรมทุกประเภทผูกพันทรัพย์สิน ตลอดจนทำนิติกรรมอื่นใดเพื่อประโยชน์ ในการดำเนินกิจการของสำนักงาน
- (3) จัดให้มีและให้ทุนเพื่อสนับสนุนการดำเนินกิจการของสำนักงาน
- (4) เรียกเก็บค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน หรือค่าบริการในการดำเนินงาน ทั้งนี้ ตามหลักเกณฑ์ และอัตราที่สำนักงานกำหนดโดยความเห็นชอบของคณะกรรมการบริหารสำนักงานคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กบส.”
- (5) ปฏิบัติการอื่นใดที่กฎหมายกำหนดให้เป็นหน้าที่และอำนาจของสำนักงาน หรือตามที่ กมช. หรือ กบส. มอบหมาย

จะเห็นได้ว่าสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งมีบทบาทสำคัญ เพื่อเตรียมความพร้อมในการป้องกัน รับมือและจัดการปัญหาภัยคุกคามทางไซเบอร์ เสริมสร้างความเข้มแข็ง ในการดูแลความมั่นคงปลอดภัยไซเบอร์ของประเทศอย่างเป็นระบบ การสร้างความรู้ ความตระหนักให้แก่ หน่วยงาน องค์กร และประชาชนทั่วไปให้สามารถดูแลตนเองได้ ตลอดจนการประสานความร่วมมือทั้งภายใน และระหว่างประเทศ

3. องค์ประกอบคณะกรรมการบริหาร

ตามมาตรา 25 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้มี คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ เรียกโดยย่อว่า “กบส.” เพื่อดูแลงานด้านกิจการบริหารงานทั่วไปของสำนักงาน โดยองค์ประกอบ กบส. ประกอบด้วย

- | | |
|--|-------------------------|
| 1) รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม | เป็นประธานกรรมการ |
| 2) ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม | เป็นกรรมการ |
| 3) อธิบดีกรมบัญชีกลาง | เป็นกรรมการ |
| 4) เลขาธิการ ก.พ. | เป็นกรรมการ |
| 5) เลขาธิการ ก.พ.ร. | เป็นกรรมการ |
| 6) กรรมการผู้ทรงคุณวุฒิจำนวนไม่เกินหกคน | เป็นกรรมการ |
| 7) เลขาธิการ | เป็นกรรมการและเลขานุการ |
| 8) พนักงานของสำนักงานที่เลขาธิการแต่งตั้งจำนวนไม่เกินสองคน | เป็นผู้ช่วยเลขานุการ |

ทั้งนี้ รายละเอียดของการแต่งตั้งและการดำรงตำแหน่งของกรรมการผู้ทรงคุณวุฒิของ กบส. ตามพระราชบัญญัติฯ กำหนด (มาตรา 25 และมาตรา 26) ซึ่งสรุปได้ดังนี้

- รัฐมนตรีที่รักษาการตามพระราชบัญญัตินี้เป็นผู้แต่งตั้งกรรมการผู้ทรงคุณวุฒิ โดยแต่งตั้งจากบุคคลซึ่งมีความรู้ ความเชี่ยวชาญและความสามารถเป็นที่ประจักษ์ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ด้านเศรษฐศาสตร์ ด้านสังคมศาสตร์ ด้านกฎหมาย ด้านบริหารธุรกิจ หรือด้านอื่นที่เกี่ยวข้อง และเป็นประโยชน์ต่อการดำเนินงานของ กบส. ตามหลักเกณฑ์และวิธีการที่ กมช. กำหนด
- กรรมการผู้ทรงคุณวุฒิใน กบส. มีวาระการดำรงตำแหน่งคราวละสี่ปี
- ในกรณีที่มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนกรรมการผู้ทรงคุณวุฒิซึ่งพ้นจากตำแหน่งก่อนวาระ รัฐมนตรีอาจแต่งตั้งกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างได้ และให้ผู้ได้รับแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิเพิ่มเติมหรือแทนตำแหน่งที่ว่างนั้นดำรงตำแหน่งได้เท่ากับวาระที่เหลืออยู่ของกรรมการผู้ทรงคุณวุฒิซึ่งได้แต่งตั้งไว้แล้ว

โดย กบส. มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) กำหนดนโยบายการบริหารงาน และให้ความเห็นชอบแผนการดำเนินงานของสำนักงาน
- (2) ออกข้อบังคับว่าด้วยการจัดองค์กร การเงิน การบริหารงานบุคคล การบริหารงานทั่วไปการพัสดุ การตรวจสอบภายใน รวมตลอดทั้งการสงเคราะห์และสวัสดิการต่าง ๆ ของสำนักงาน
- (3) อนุมัติแผนการใช้จ่ายเงินและงบประมาณรายจ่ายประจำปีของสำนักงาน
- (4) ควบคุมการบริหารงานและการดำเนินการของสำนักงานและเลขาธิการ ให้เป็นไปตามพระราชบัญญัตินี้ และกฎหมายอื่นที่เกี่ยวข้อง
- (5) วินิจฉัยคำสั่งทางปกครองของเลขาธิการในส่วนที่เกี่ยวกับการบริหารงานของสำนักงาน
- (6) ประเมินผลการดำเนินงานของสำนักงานและการปฏิบัติงานของเลขาธิการ
- (7) ปฏิบัติหน้าที่อื่นตามที่พระราชบัญญัตินี้หรือกฎหมายอื่นกำหนดให้เป็นหน้าที่และอำนาจของ กบส. หรือตามที่คณะกรรมการหรือคณะรัฐมนตรีมอบหมายในการปฏิบัติงาน

ทั้งนี้ กบส. อาจแต่งตั้งคณะอนุกรรมการเพื่อพิจารณา เสนอแนะหรือกระทำการอย่างหนึ่งอย่างใดตามที่ กบส. มอบหมายได้

คณะกรรมการบริหารสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

จำนวนไม่เกิน 6 คน

วาระการดำรงตำแหน่งคราวละ 4 ปี
(คณะรัฐมนตรีเป็นผู้แต่งตั้ง)

1. ด้านการรักษามั่นคงปลอดภัยไซเบอร์
2. ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
3. ด้านเศรษฐกิจ
4. ด้านสังคมศาสตร์
5. ด้านกฎหมาย
6. ด้านบริหารธุรกิจ
7. ด้านอื่นที่เกี่ยวข้อง

รัฐมนตรีว่าการกระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม
ประธานกรรมการ

กรรมการผู้ทรงคุณวุฒิ

กรรมการโดยตัวแทน

จำนวน 4 คน

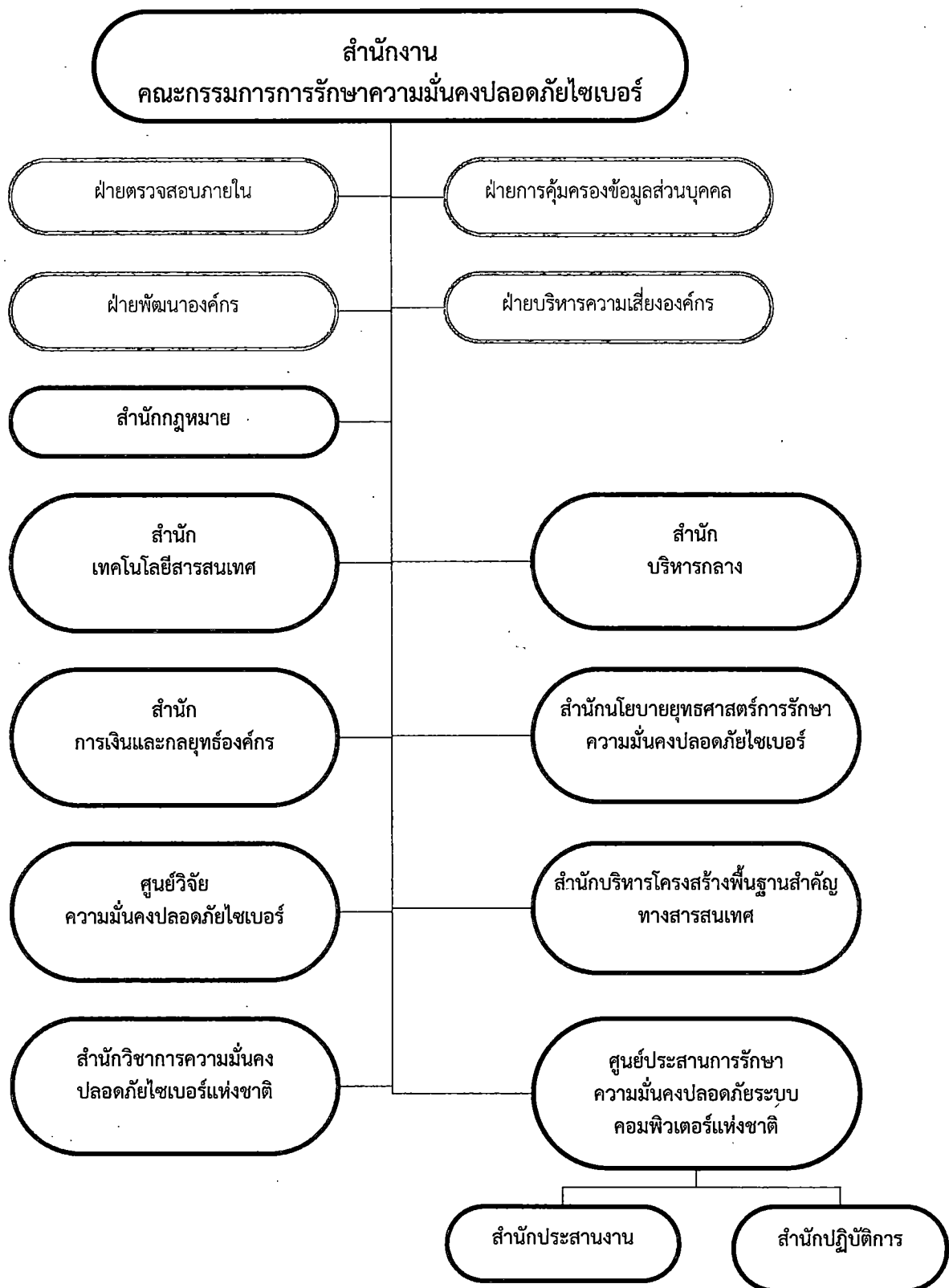
1. ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
2. อธิบดีกรมบัญชีกลาง
3. เลขาธิการ ก.พ.
4. เลขาธิการ ก.น.ร.

พนักงานของสำนักงาน
จำนวนไม่เกิน 2 คน
(เลขานุการแต่งตั้ง)

ผู้ช่วยเลขานุการ

เลขานุการ
กรรมการและเลขานุการ

4. โครงสร้างสำนักงาน



โดยโครงสร้างของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งประกอบด้วย

1) หน่วยงานที่ขึ้นตรงกับเลขาธิการ ประกอบด้วย 4 ฝ่าย ดังนี้

1.1) ฝ่ายตรวจสอบภายใน

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) จัดทำแผนการตรวจสอบภายในภาพรวมของสำนักงานและแผนการตรวจสอบประจำปี
- (2) ตรวจสอบการดำเนินงานภายในสำนักงาน และ เสนอแนะ ให้คำปรึกษา เพื่อปรับปรุงแก้ไขการดำเนินงานแก่หน่วยรับตรวจ
- (3) ดำเนินการเกี่ยวกับการตรวจสอบด้านการบริหาร การเงิน และการบัญชีของสำนักงาน และ รายงานผลให้เลขาธิการคณะกรรมการฯ ทราบ
- (4) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง หรือที่ได้รับมอบหมาย

1.2) ฝ่ายการคุ้มครองข้อมูลส่วนบุคคล

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) ให้คำแนะนำ และตรวจสอบ แก่ผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล ของสำนักงาน รวมทั้ง ลูกจ้างหรือผู้รับจ้างของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลเกี่ยวกับการปฏิบัติตามกฎหมาย การคุ้มครองข้อมูลส่วนบุคคล
- (2) ตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูล หรือผู้ประมวลผลข้อมูล รวมทั้งลูกจ้างหรือผู้รับจ้าง ของผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลเกี่ยวกับการเก็บรวบรวม การใช้หรือการเปิดเผย ข้อมูลเพื่อให้เป็นไปตามกฎหมายการคุ้มครองข้อมูลส่วนบุคคล
- (3) รักษาความลับและคุ้มครองข้อมูลส่วนบุคคลที่สำนักงานล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ ตามกฎหมายการคุ้มครองข้อมูลส่วนบุคคล
- (4) ประสานงาน และรับเรื่องร้องเรียน แก้ไขปัญหา รวมถึงให้ความร่วมมือหน่วยงานที่เกี่ยวข้อง
- (5) ดำเนินการต่างๆ ให้สอดคล้องกับกฎหมายการคุ้มครองข้อมูลส่วนบุคคล

1.3) ฝ่ายพัฒนาองค์กร

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) เสนอแนะและให้คำปรึกษาแก่เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัย ไซเบอร์แห่งชาติเกี่ยวกับยุทธศาสตร์การพัฒนาระบบบริหารสำนักงาน
- (2) ติดตาม ประเมินผล และจัดทำรายงานเกี่ยวกับการพัฒนาระบบบริหารสำนักงาน
- (3) ประสานและดำเนินการเกี่ยวกับการพัฒนาระบบบริหาร ร่วมกับหน่วยงานกลางต่างๆ และ หน่วยงานภายในสำนักงาน
- (4) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง หรือที่ได้รับมอบหมาย

1.4) ฝ่ายบริหารความเสี่ยงองค์กร

มีหน้าที่และอำนาจ ดังต่อไปนี้

จัดทำแผนการบริหารความเสี่ยงขององค์กรให้เป็นไปในทิศทางที่สอดคล้องกับผลการดำเนินงานของ องค์กร และเสนอแนะการเตรียมความพร้อมเพื่อรองรับปัจจัยเสี่ยงจากทั้งภายในและภายนอกที่จะ ส่งผลกระทบต่อองค์กร

2) สำนักกฎหมาย

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) พัฒนา ปรับปรุงกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์
- (2) ดำเนินการเกี่ยวกับงานนิติกรรมและสัญญา รวมทั้งให้การสนับสนุนเกี่ยวกับงานด้านกฎหมาย ในการดำเนินการตามข้อตกลงความร่วมมือหรืออนุสัญญาของสำนักงาน
- (3) ดำเนินการตรวจสอบ สืบสวนและสอบสวน และอื่นๆ ที่เกี่ยวข้องกับการงานด้านวินัย อุทธรณ์ และร้องทุกข์
- (4) ดำเนินงานที่เกี่ยวกับความรับผิดชอบทางแพ่งและอาญา งานคดีปกครอง และงานคดีอื่นที่อยู่ในหน้าที่และอำนาจของสำนักงาน
- (5) ดำเนินการเกี่ยวกับงานกฎหมาย กฎ ระเบียบที่เกี่ยวข้อง รวมถึงงานที่เกี่ยวกับความรับผิดชอบทางแพ่งและอาญา งานคดีปกครอง ตลอดจนดำเนินการทางปกครอง และเป็นศูนย์กลางข้อมูลคดีของสำนักงาน
- (6) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง หรือที่ได้รับมอบหมาย

3) สำนักเทคโนโลยีสารสนเทศ

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) เชื่อมโยงระบบเครือข่ายสารสนเทศของสำนักงานและหน่วยงานอื่นๆ ที่เกี่ยวข้อง รวมทั้ง จัดทำระบบสิ่งอำนวยความสะดวกด้านสารสนเทศ ให้กับหน่วยงานๆ ภายในสำนักงาน และบริหารจัดการอุปกรณ์ Hardware Software และระบบของสำนักงาน
- (2) พัฒนาและบำรุงรักษาระบบเทคโนโลยีสารสนเทศ ที่จำเป็นสำหรับการดำเนินงานของสำนักงาน ระบบสารสนเทศ ระบบฐานข้อมูลให้ทันสมัย รวมทั้งให้คำปรึกษาแนะนำการใช้งาน
- (3) จัดทำนโยบายและแนวปฏิบัติ รวมถึงดำเนินการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของสำนักงาน
- (4) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

4) สำนักบริหารกลาง

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) บริหารจัดการงานทั่วไป งานธุรการ งานสารบรรณ งานเอกสาร และ งานพัสดุ
- (2) ดำเนินการ และสนับสนุนการจัดประชุมอันเกี่ยวเนื่องกับกิจการของสำนักงานหรือตามที่ได้รับมอบหมาย
- (3) บริหารจัดการงานเลขานุการ ให้แก่ ผู้บริหารขององค์กร
- (4) เสนอแนะนโยบาย กลยุทธ์ และจัดทำแผนบริหารจัดการทรัพยากรบุคคล การปรับปรุงระเบียบข้อบังคับ
- (5) เสนอแนะนโยบาย กลยุทธ์ และจัดทำแผนพัฒนาทรัพยากรบุคคล เพื่อพัฒนาทักษะ ชีตความสามารถของบุคคลอย่างต่อเนื่อง รวมถึงการจัดกิจกรรมสัมพันธ์สำหรับบุคลากรในองค์กร
- (6) ดำเนินการที่เกี่ยวข้องกับการสรรหาบุคคล การบริหารงานบุคคล และพัฒนาทรัพยากรบุคคล
- (7) ดำเนินการเกี่ยวข้องกับการประเมินผลการปฏิบัติงานของพนักงานและลูกจ้างของสำนักงาน ตามข้อบังคับของ กบส. และระเบียบของสำนักงาน

- (8) เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างความรู้ความตระหนักด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการ ดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน
- (9) เสริมสร้างความรู้ความเข้าใจเกี่ยวกับงานและภาพลักษณ์ที่ดี และเสริมสร้างกิจกรรมเชิงสร้างสรรค์ต่อประชาชน หน่วยงานภายนอกต่างๆ ให้มีทัศนคติอันดีต่อองค์กร
- (10) ส่งเสริม สนับสนุน การดำเนินการในการเผยแพร่ความรู้ และผลิตสื่อประชาสัมพันธ์เชิงสร้างสรรค์ในรูปแบบต่างๆ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้ง การเผยแพร่ผลการดำเนินงานประจำปี
- (11) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

5) สำนักการเงินและกลยุทธ์องค์กร

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) บริหารจัดการเกี่ยวกับทุนและทรัพย์สินเพื่อสนับสนุนการดำเนินกิจการของสำนักงานเงินสงเคราะห์ และสวัสดิการต่างๆ ของสำนักงาน
- (2) กำกับ และติดตามการใช้จ่ายเงินและงบประมาณให้เป็นไปตามแผนการใช้จ่ายประจำปีของสำนักงาน
- (3) ดำเนินการจัดการเกี่ยวกับ ค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน หรือค่าบริการต่างๆ เงินรายได้ อันเกิดจากการดำเนินการตามหน้าที่และอำนาจของสำนักงาน และดอกผลของเงินหรือรายได้จากทรัพย์สินของสำนักงาน
- (4) ดำเนินการจัดท่างบการเงินและบัญชี แล้วส่งผู้สอบบัญชีภายในเก้าสิบวันนับแต่วันสิ้นปีบัญชี
- (5) กำหนดทิศทางการขับเคลื่อนและการจัดการเชิงกลยุทธ์ขององค์กร
- (6) จัดทำแผนปฏิบัติราชการของตามแผนกลยุทธ์ให้เป็นไปในทิศทางที่สอดคล้องกับนโยบายระดับชาติ ดำเนินการพัฒนา ทบทวน ปรับปรุง แผนปฏิบัติราชการประจำปี เพื่อให้เป็นแนวปฏิบัติเพื่อให้เกิดผลสำเร็จ
- (7) จัดทำแผนงบประมาณ และจัดสรรงบประมาณรายจ่ายประจำปี ให้เป็นไปในทิศทางที่สอดคล้องกับเป้าหมายขององค์กร
- (8) ขับเคลื่อนยุทธศาสตร์ นโยบาย และแผนงาน การจัดสรรงบประมาณขององค์กรตลอดจนโครงการพิเศษ
- (9) ดำเนินการติดตาม ประเมินผล และจัดทำรายงานเกี่ยวกับการพัฒนาระบบบริหารภายในสำนักงาน
- (10) ติดตาม พัฒนา และปรับปรุงการจัดการและการบริหารงานทั่วไปของสำนักงานให้มีประสิทธิภาพตามที่ได้รับมอบหมาย
- (11) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

6) สำนักนโยบายยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) จัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์
- (2) จัดทำนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

- (3) จัดทำ และกำกับดูแล แผนแม่บท และแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ ในสถานการณ์ปกติและสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์
- (4) วิเคราะห์ ติดตาม และประเมินผลการดำเนินงานของโครงการตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- (5) ปฏิบัติ ประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบาย และแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
- (6) รายงานความคืบหน้าและสถานการณ์ รวมทั้งปัญหาและอุปสรรค เกี่ยวกับการปฏิบัติตามนโยบาย และแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์แผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- (7) ติดตาม ประเมินผล และจัดทำสรุปผลการดำเนินการของสำนักงานประจำปี
- (8) กำหนดแนวทาง มาตรการ และกำกับดูแลการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- (9) จัดทำมาตรฐานสำหรับการรายงาน และกำกับดูแลการดำเนินการการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามมาตรฐานที่กำหนด
- (10) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

7) ศูนย์วิจัยข้อมูลความมั่นคงปลอดภัยไซเบอร์

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) ศึกษา วิจัยและพัฒนาเทคโนโลยีและองค์ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- (2) ศึกษา วิจัย และจัดทำฐานข้อมูลสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์
- (3) รวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและเอกชน
- (4) ศึกษาวิจัย รวบรวมและวิเคราะห์ข้อมูลด้านเทคโนโลยีของการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อกำหนดและรับรองมาตรฐาน
- (5) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

8) สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ สร้างมาตรฐานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน
- (2) จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและ

- หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุที่ส่งผลกระทบหรือ ก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรือร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้ การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน
- (3) กำหนดหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน้าที่ของหน่วยงานควบคุมหรือ กำกับดูแล โดยอย่างน้อยต้องกำหนดหน้าที่ให้หน่วยงานควบคุมหรือกำกับดูแลต้องกำหนดมาตรฐานที่ เหมาะสมเพื่อรับมือกับภัยคุกคามทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ
 - (4) กำหนดลักษณะหน่วยงานที่มีภารกิจหรือบริการที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
 - (5) ประสานงานและให้ความร่วมมือให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดตั้งศูนย์ประสาน การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคง ปลอดภัยไซเบอร์และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์
 - (6) กำหนดหลักเกณฑ์และวิธีการการรายงาน เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อ ระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
 - (7) วิเคราะห์ปัญหา อุปสรรค และรายงานผลการดำเนินการพระราชบัญญัติการรักษาความมั่นคงปลอดภัย ไซเบอร์ และสถานภาพความพร้อมตามมาตรฐานสากลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
 - (8) ประสาน สนับสนุน ให้ความช่วยเหลือ กำกับดูแล และติดตาม หน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศให้ดำเนินการจัดทำและปฏิบัติตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
 - (9) ส่งเสริม สนับสนุน จัดการฝึกอบรมและเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคาม ไซเบอร์ร่วมกับหน่วยงานที่เกี่ยวข้อง รวมถึงกิจกรรมต่างๆ เพื่อเตรียมความพร้อมในการรับมือกับภัย คุกคามทางไซเบอร์
 - (10) จัดการฝึกเพื่อประเมินความพร้อมในการรับมือกับภัยคุกคามไซเบอร์ของหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ
 - (11) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

9) สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) ส่งเสริม สนับสนุน และดำเนินการฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- (2) กำหนดมาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ของพนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ หน่วยงานของรัฐหน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้อง กับการรักษาความมั่นคงปลอดภัยไซเบอร์
- (3) ศึกษา วิจัย และจัดทำองค์ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- (4) จัดทำแผน และหลักสูตรการฝึกอบรมสำหรับบุคลากรด้านไซเบอร์
- (5) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

10) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

10.1) สำนักประสานงาน

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) ประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์
- (2) ประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ
- (3) จัดทำความตกลงและร่วมมือกับองค์กรหรือหน่วยงานทั้งในประเทศและต่างประเทศ ในกิจการที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน
- (4) อำนาจความสะดวกในการประสานงานระหว่างหน่วยงานของรัฐที่เกี่ยวข้องและหน่วยงานเอกชนเพื่อจัดการความเสี่ยงและเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
- (5) เป็นศูนย์กลางเครือข่ายข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศทั้งข้อมูลภายในและต่างประเทศ โดยการประสานงานกับหน่วยงานของรัฐ และเอกชน เพื่อรวบรวมและวิเคราะห์ข้อมูล เกี่ยวกับภัยคุกคามการป้องกัน การรับมือความเสี่ยงจากสถานการณ์ด้านภัยคุกคามไซเบอร์ และข้อมูลอื่นใด อันเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- (6) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

10.2) สำนักปฏิบัติการ

มีหน้าที่และอำนาจ ดังต่อไปนี้

- (1) เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์
- (2) กำหนดระดับของภัยคุกคามทางไซเบอร์ พร้อมทั้งรายละเอียดของมาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ
- (3) วิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์ ทำรายงานผลต่อคณะกรรมการพิจารณาสั่งการ เมื่อมีหรือคาดว่าจะมีภัยคุกคามไซเบอร์ในระดับที่ร้ายแรงขึ้น
- (4) กำหนดลักษณะของภัยคุกคามทางไซเบอร์ และกลไกหรือขั้นตอนเพื่อการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- (5) กำหนดหลักเกณฑ์และวิธีการการรายงาน เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- (6) ประสานความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- (7) ประสานให้ความช่วยเหลือด้านบุคลากรหรือเทคโนโลยีแก่หน่วยงานนั้นตามที่ร้องขอได้ในกรณีที่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่อาจดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- (8) รวบรวมข้อมูล หรือพยานเอกสาร พยานบุคคล พยานวัตถุที่เกี่ยวข้อง เพื่อวิเคราะห์สถานการณ์ และประเมินผลกระทบจากภัยคุกคามทางไซเบอร์
- (9) เสนอความเห็น วิเคราะห์ วางแผน ประสานงาน และดำเนินการเกี่ยวกับ การรับมือเหตุการณ์ทางไซเบอร์ ประกอบด้วย การเตรียมการ (Preparation) การตรวจจับและวิเคราะห์ (Detection and Analysis) การกักกัน กำจัด และกู้คืน (Containment, Eradication, and Recovery) และการดำเนินการหลังเหตุการณ์ (Post-Incident Activity)
- (10) ตอบสนองและรับมือภัยคุกคามไซเบอร์ เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัยหรือสถานการณ์ ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดที่ส่งผลกระทบ หรืออาจก่อให้เกิดผลกระทบ ความสูญเสีย หรือ ความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรง โดยวางมาตรการเกี่ยวกับการดำเนินการ ที่คำนึงถึงชั้นความลับและการเข้าถึงข้อมูลที่มีชั้นความลับ โดยประสานความร่วมมือทางปฏิบัติในการ ดำเนินการกับหน่วยงานภาครัฐหรือหน่วยงานเอกชน เพื่อให้การยับยั้งปัญหาภัยคุกคามไซเบอร์ได้รับการแก้ไข อย่างมีประสิทธิภาพและรวดเร็ว รวมถึงการติดตามผลการปฏิบัติงาน การแก้ไขสถานการณ์เพื่อให้กลับคืนสู่ สภาพปกติโดยเร็ว
- (11) จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยยะสำคัญหรือแนวทางการพัฒนามาตรการรักษาความมั่นคงปลอดภัยไซเบอร์
- (12) ป้องกันเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดจากภัยคุกคามทางไซเบอร์ เสนอแนะหรือสั่งการให้ใช้ระบบที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการหาแนวทางตอบโต้หรือการแก้ไขปัญหาเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
- (13) ประสานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องเพื่อรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง
- (14) ประสานงาน สนับสนุน และให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ หรือตามคำสั่งของคณะกรรมการ
- (15) ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือที่ได้รับมอบหมาย

5. อัตรากำลัง

การประชุมคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กบส.) ครั้งที่ 1/2563 เมื่อวันที่ 8 กันยายน 2563 กบส. ได้พิจารณากรอบโครงสร้างและอัตรากำลังของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดย กบส. ได้เห็นชอบภาพรวมของกรอบโครงสร้างและอัตรากำลังของสำนักงาน และเพื่อให้เกิดความยืดหยุ่นของกรอบโครงสร้างและอัตรากำลังของสำนักงานฯ โดยภายใต้โครงสร้างและกรอบอัตรากำลังของสำนักงานสามารถปรับเปลี่ยนได้ตามความเหมาะสม และเพื่อความสะดวกต่อการบริหารงาน ดังนี้

ตำแหน่ง/หน่วยงาน	อัตรา (คน)
เลขาธิการ	1
รองเลขาธิการ	4
ผู้ช่วยเลขาธิการ	3
ผู้ทรงคุณวุฒิ	2
1. ฝ่ายงานที่ขึ้นตรงเลขาธิการ	
1.1 ฝ่ายตรวจสอบภายใน	2
1.2 ฝ่ายการคุ้มครองข้อมูลส่วนบุคคล	3
1.3 ฝ่ายพัฒนาองค์กร	3
1.4 ฝ่ายบริหารความเสี่ยงองค์กร	3
2. สำนักกฎหมาย	20
3. สำนักเทคโนโลยีสารสนเทศ	22
4. สำนักบริหารกลาง	44
5. สำนักการเงินและกลยุทธ์องค์กร	31
6. สำนักนโยบายยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	48
7. ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์	44
8. สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	61
9. สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	60
10. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	
10.1 สำนักประสานงาน	61
10.2 สำนักปฏิบัติการ	68
รวมทั้งสิ้น	480

6. ความยากง่ายหรือความยุ่งยากซับซ้อนของภารกิจ

6.1 สถานการณ์และแนวโน้มของภัยคุกคามทางไซเบอร์

(1) แนวโน้มของปัญหาภัยคุกคามไซเบอร์เพิ่มขึ้นอย่างต่อเนื่อง และประเทศไทยยังขาดหน่วยงานกลางในการดูแลและรับมือกับภัยคุกคามไซเบอร์

ความก้าวหน้าทางเทคโนโลยีที่เพิ่มขึ้น และการใช้ประโยชน์ของเทคโนโลยีเป็นเครื่องมือในการดำเนินชีวิต เป็นสิ่งที่ขับเคลื่อนเศรษฐกิจในกิจกรรมต่างๆ อย่างมากมาย ส่งผลให้ปัญหาของภัยคุกคามไซเบอร์มีรูปแบบที่หลากหลาย ซับซ้อน และทวีความรุนแรงยิ่งขึ้น โดยเฉพาะภัยคุกคามไซเบอร์ที่มีแนวโน้มส่งผลกระทบต่อเศรษฐกิจ เช่น WannaCry ที่เป็นตัวอย่างของ Ransomware ซึ่งกระทบต่อระบบของทั่วโลกในหลายๆ ภาคส่วน จากความตระหนักในด้านความเสถียรบนโลกอินเทอร์เน็ตที่ทวีความรุนแรงมากขึ้นเรื่อยๆ อันเนื่องมาจากภัยคุกคามทางไซเบอร์ที่ซับซ้อนมีการขยายตัวเพิ่มมากขึ้น ซึ่งแน่นอนว่าย่อมส่งผลกระทบต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือ “Critical Information Infrastructure (CII)” ของประเทศ ที่มีการใช้งานคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ซึ่งหากถูกโจมตีจากภัยคุกคามทางไซเบอร์แล้ว จะส่งผลกระทบต่อความสูญเสียอย่างร้ายแรงต่อประเทศอย่างมาก ทั้งในด้านเศรษฐกิจ สังคม การดำเนินชีวิตประจำวันของประชาชน ไปจนถึงความมั่นคงของชาติ

อีกทั้ง เมื่อปัญหาการโจมตีทางด้านไซเบอร์ มีจำนวนเพิ่มขึ้น อันเนื่องมาจากสภาพแวดล้อมการใช้เทคโนโลยีสารสนเทศที่ไม่มีความมั่นคงปลอดภัย ความไว้วางใจและความเชื่อมั่นย่อมได้รับผลกระทบอย่างมีนัยสำคัญ จึงเป็นเหตุผลสำคัญที่จำเป็นต้องมีหน่วยงานกลางในระดับชาติเพื่อประสานความร่วมมือรองรับสถานการณ์ดังกล่าว

และด้วยภารกิจด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มีความซับซ้อน หลากหลายและครอบคลุมในหลายมิติ ปัจจัยสำคัญประการหนึ่งสืบเนื่องมาจากการพัฒนาทางเทคโนโลยี และการขาดความตระหนักและความรู้ความเข้าใจ เกี่ยวกับการดูแลและใส่ใจต่อความมั่นคงปลอดภัยไซเบอร์ของผู้ใช้งาน ดังนั้น เพื่อให้การดำเนินการกิจตามพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นต้องผลักดันการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อเป็นหน่วยงานกลางที่จะสร้างกลไกในการขับเคลื่อนการทำงานในการดูแลและรับมือภัยคุกคามไซเบอร์ รวมทั้งให้ความช่วยเหลือและสนับสนุนหน่วยงานภาครัฐ และหน่วยงานที่เป็นพื้นฐานสำคัญทางสารสนเทศเพื่อลดความเสี่ยงและบรรเทาความเสียหายจากภัยคุกคามที่จะเกิดขึ้น ซึ่งในการดำเนินงานดังกล่าวต้องอาศัยผู้เชี่ยวชาญเฉพาะด้าน และมีกลไกการทำงานที่มีความคล่องตัวพร้อมสำหรับการปฏิบัติงานทั้งด้านนโยบาย เทคโนโลยี การวิจัยพัฒนา และกฎหมาย ที่สามารถสนับสนุนการทำงานของคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

(2) ยกระดับความเชื่อมั่นด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของไทย

เมื่อเปรียบเทียบ ระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยกับต่างประเทศ ในปี พ.ศ. 2561 สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union : ITU) ได้ทำการสำรวจระดับความเอาใจจริงเอาใจ (Commitment) ด้านความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ โดยพิจารณาจากมาตรการ 5 ด้าน ได้แก่ ด้านกฎหมาย (Legal) ด้านเทคนิค (Technical) ด้านหน่วยงาน/นโยบาย

(Organizational) ด้านการพัฒนาศักยภาพ (Capacity building) และด้านความร่วมมือ (Cooperation) ประกอบด้วย 17 ปัจจัยย่อย ดังนี้

ปัจจัยหลัก	ปัจจัยย่อย
1. มาตรการทางกฎหมาย (Legal Measures)	1.1 กฎหมายอาญา (Criminal Legislation) ที่เกี่ยวกับการควบคุมการกระทำความผิดทางคอมพิวเตอร์ 1.2 การมีกฎระเบียบและการปฏิบัติตามกฎระเบียบ (Regulation and Compliance) หมายถึง การมีกฎที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์เฉพาะเรื่อง เช่น กฎหมายการใช้ลายเซ็นอิเล็กทรอนิกส์ เป็นต้น
2. มาตรการทางเทคนิค (Technical Measures)	2.1 การจัดตั้งหน่วยงานระดับชาติเพื่อตอบสนองเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยทางไซเบอร์ (CIRT (Computer Incident Response Team), Cyber Protection Team (CPT), CERT (Computer Emergency Response Team) หรือ CSIRT (Computer Security Incident Response Team)) 2.2 มาตรฐาน (Standards) 2.3 การออกใบรับรอง (Certifications)
3. มาตรการด้านโครงสร้างองค์กร (Organizational Measures)	3.1 นโยบาย (Policy) 3.2 แผนด้านการกำกับดูแล (Roadmap for Governance) 3.3 หน่วยงานผู้รับผิดชอบ (Responsible Agency) 3.4 การเทียบเคียงกับหน่วยงานระดับชาติ (National Benchmarking)
4. การพัฒนาศักยภาพบุคลากร (Capacity Building)	4.1 การกำหนดมาตรฐานในการพัฒนาบุคลากร (Standardization Development) 4.2 การพัฒนาบุคลากร (Manpower Development) 4.3 การให้การรับรองแก่ผู้เชี่ยวชาญ (Professional Certification) 4.4 การให้การรับรองหน่วยงาน (Agency Certification)
5. การสร้างความร่วมมือ (Cooperation)	5.1 การสร้างความร่วมมือระหว่างรัฐ (Intra-State Cooperation) 5.2 การสร้างความร่วมมือระหว่างหน่วยงาน (Intra-Agency Cooperation) 5.3 ความร่วมมือภาครัฐและภาคเอกชน (Public-private partnerships (PPP)) 5.4 การสร้างความร่วมมือระหว่างประเทศ (International Cooperation)

ซึ่งพบว่า ดัชนีความมั่นคงปลอดภัยไซเบอร์โลก (Global Cybersecurity Index : GCI) ของ ITU โดยในปี พ.ศ. 2561 (ค.ศ. 2018) ประเทศไทยอยู่ในอันดับที่ 35 (บางระดับอันดับซ้ำกัน) จาก 194 ประเทศ โดยที่เมื่อปี พ.ศ. 2560 (ค.ศ. 2017) ประเทศไทยอยู่ในอันดับที่ 22 นอกจากนี้ เมื่อเปรียบเทียบกับประเทศสมาชิกในกลุ่มอาเซียนแล้ว ประเทศไทยอยู่อันดับที่ 3 รองจากสิงคโปร์ และมาเลเซีย ซึ่งมาตรการด้านหนึ่งที่ต้องเร่งผลักดันเนื่องจากยังอยู่ในระดับที่น่าเป็นห่วง คือ การมีหน่วยงานเพื่อดำเนินภารกิจด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ของประเทศโดยตรง ดังนั้น เพื่อเป็นการยกระดับการจัดอันดับความพร้อมด้าน

ความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ซึ่งการจัดตั้งสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติตามพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จึงเป็นเรื่องที่มีความจำเป็นและเร่งด่วน

ประกอบกับ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่ 12 พ.ศ. 2560 – 2564 ได้เล็งเห็นถึงความสำคัญของภัยคุกคามทางไซเบอร์ที่เพิ่มระดับความรุนแรงและมีความซับซ้อนในการโจมตีมากขึ้น ความเสียหายที่เกิดจากการอาชญากรรมและการโจมตีทางไซเบอร์จะมีผลอย่างร้ายแรง ซึ่งต้องให้ความสำคัญและมีการป้องกันภัยคุกคามทางไซเบอร์ให้สอดคล้องกับการเปลี่ยนแปลงทางสภาพแวดล้อม โดยเฉพาะการกำหนดกฎหมายและมาตรการที่เกี่ยวกับความปลอดภัยบนโลกไซเบอร์ให้รัดกุมมากยิ่งขึ้นตั้งแต่ระดับชาติถึงระดับบุคคล โดยได้กำหนดไว้ในยุทธศาสตร์ที่ 5 “การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่นคงและยั่งยืน” เป้าหมายที่ 5 “ประเทศไทยมีความพร้อมต่อการรับมือภัยคุกคามทั้งภัยคุกคามทางทหารและภัยคุกคามอื่นๆ” ซึ่งได้กำหนดตัวชี้วัดสำคัญ คือ “อันดับความเสี่ยงจากการโจมตีด้านไซเบอร์/ต่ำกว่าอันดับที่ 10 ของโลก (ดัชนีความปลอดภัยไซเบอร์ของโลกของ International Telecommunication Union: ITU)” ด้วยเหตุนี้ หากประเทศไทยมีการผลักดันความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยตามแนวทางมาตรการ 5 ด้าน ได้แก่ ด้านกฎหมาย (Legal) ด้านเทคนิค (Technical) ด้านหน่วยงาน/นโยบาย (Organizational) ด้านการพัฒนาศักยภาพ (Capacity building) และด้านความร่วมมือ (Cooperation) อย่างจริงจัง ก็จะส่งผลให้ประเทศไทยสามารถอยู่ในอันดับความเสี่ยงจากการโจมตีด้านไซเบอร์/ต่ำกว่าอันดับที่ 10 ของโลกตามเป้าหมายตัวชี้วัดที่ได้กำหนดไว้ในแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่สิบสอง พ.ศ. 2560 – 2564 ได้

จากสถานการณ์ดังกล่าว ประกอบกับประเทศไทยยังขาดบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์จำนวนมาก และต้องการเตรียมความพร้อมเพื่อรองรับภัยคุกคามจำนวนมากในอนาคต จึงเป็นนโยบายหลักของรัฐที่ต้องเร่งดำเนินการเพื่อป้องกันการโจมตีทางไซเบอร์ของประเทศไทย ซึ่งจากผลการวิจัยระหว่างบริษัท พรอสต์ แอนด์ ซัลลิแวน (ประเทศไทย) จำกัด กับ บริษัท ไมโครซอฟท์ (ประเทศไทย) จำกัด พบว่าผลกระทบจากการถูกโจมตีทางไซเบอร์ของประเทศไทย จะเกิดความเสียหายทางเศรษฐกิจในประเทศไทยที่เป็นผลกระทบมาจากการถูกโจมตีทางไซเบอร์สูงถึง 2.86 แสนล้านบาทหรือ เท่ากับร้อยละ 2.2 ของผลิตภัณฑ์มวลรวมของประเทศ ทั้งนี้ พบว่า 3 ใน 5 ขององค์กรในประเทศไทยเคยได้รับผลกระทบจากการถูกโจมตีทางไซเบอร์ ดังนั้น บทบาทของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจึงมีความสำคัญอย่างมากต่อเศรษฐกิจของประเทศและนโยบายรัฐบาล

6.2 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นองค์การมหาชนที่จัดตั้งขึ้นเพื่อพัฒนาและดำเนินการตามนโยบายสำคัญเฉพาะด้านของรัฐให้เกิดผลในทางปฏิบัติภายในระยะเวลาจำกัด

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจัดตั้งขึ้นรองรับนโยบายเฉพาะของรัฐบาล และยุทธศาสตร์ชาติ ระยะ 20 ปี แผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง ในส่วนของ “การป้องกันและแก้ไขปัญหาด้านความมั่นคงทางไซเบอร์” มุ่งเน้นการวางกลยุทธ์/ยุทธวิธีในการแก้ไขปัญหาด้านความมั่นคงทางไซเบอร์ ให้ครอบคลุมสภาพปัญหาของภัยคุกคามทางไซเบอร์ เช่น การโจมตีทางไซเบอร์ของกลุ่มแฮกเกอร์ การโจมตีต่อกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศ อันกระทบต่อประชาชน รวมทั้งอาจส่งผลกระทบต่อความมั่นคง โดยแผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง ได้กำหนดแนวคิดในการดำเนินการ

แก้ไขปัญหที่สำคัญ ประกอบด้วย (1) กำหนดแนวความคิด มาตรการ มาตรฐาน ระบบบริหารจัดการในการป้องกันและแก้ไขปัญหความมั่นคงทางไซเบอร์ในภาพรวม (2) จัดองค์กร โครงสร้าง อำนาจหน้าที่ ขีดความสามารถในการป้องกันและแก้ไขปัญหความมั่นคงทางไซเบอร์ (3) กำหนดระบบบริหารจัดการในแต่ละระดับให้ชัดเจน (4) เสริมสร้างและพัฒนาระบบการรายงานในสถานการณ์ฉุกเฉิน (5) ยกระดับแนวความคิดในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (6) พัฒนาการป้องกันแก้ไขปัญหการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคง (7) สร้างความตระหนักรู้ให้แก่ประชาชนและหน่วยงาน (8) ปรับปรุงแก้ไขกฎหมายที่เกี่ยวข้อง และ (9) พัฒนาศักยภาพบุคลากรและเทคโนโลยีให้ทันสมัยพร้อมรองรับสถานการณ์ทุกรูปแบบ อีกทั้ง ยังสอดคล้องกับแผนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560-2564 คือ 1) การปกป้อง โครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ 2) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ 3) การบูรณาการการจัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ 4) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ 5) การสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ 6) การพัฒนากฎหมาย ระเบียบ และมาตรฐาน เพื่อความมั่นคงปลอดภัยไซเบอร์ 7) การประสานความร่วมมือระหว่างประเทศเพื่อความมั่นคงปลอดภัยไซเบอร์ 8) การวิจัยและพัฒนาเพื่อความมั่นคงปลอดภัยไซเบอร์

ทั้งนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้มีการจัดทำแผนปฏิบัติการระยะ 3 ปี (พ.ศ. 2563 - 2565) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีวัตถุประสงค์เพื่อใช้เป็นกรอบแนวทางการดำเนินงานของหน่วยงานภายในสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการพัฒนาองค์กรเพื่อขับเคลื่อนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และสอดคล้องกับยุทธศาสตร์ชาติ ระยะ 20 ปี แผนแม่บทภายใต้ยุทธศาสตร์ชาติ แผนการปฏิรูปประเทศ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2562-2565) นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561 - 2580) แผนปฏิบัติการด้านดิจิทัลเพื่อเศรษฐกิจและสังคมระยะ 5 ปี (พ.ศ. 2562 - 2565) ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560 - 2564) และแผนเตรียมพร้อมแห่งชาติ (พ.ศ. 2560 - 2564) โดยแผนปฏิบัติการระยะ 3 ปี (พ.ศ. 2563 - 2565) ของสำนักงานฯ ซึ่งเป็นการจัดทำแผนปฏิบัติการของส่วนราชการ ให้จัดทำเป็นแผนสามปีโดยมีห้วงระยะเวลาตั้งแต่ปีงบประมาณ พ.ศ. 2563 ถึงปีงบประมาณ พ.ศ. 2565 ตามมาตรา 9 ของพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และการบริหารกิจการบ้านเมืองที่ดี (ฉบับที่ 2) พ.ศ. 2562 กำหนดไว้ โดยเป็นการกำหนดแผนงานโครงการสำคัญที่ครอบคลุมระยะเวลาการดำเนินงานในระยะ 3 ปี คือ พ.ศ. 2563 - 2565 เพื่อช่วยให้เห็นภาพรวมของแนวทางการพัฒนาสู่การดำเนินการของหน่วยงานอย่างเป็นระบบ เพื่อการพัฒนาประเทศให้มีความมั่นคงและมีขีดความสามารถในการรับมือต่อภัยคุกคามทางไซเบอร์ในทุกมิติ ดังนี้

ในปีที่ 1 มุ่งเน้นการจัดตั้งสำนักงานฯ เพื่อใช้เป็นกลไกหลักสำคัญในการพัฒนางานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยจะสรรหาและบรรจุแต่งตั้งบุคลากรผู้มีความรู้ความสามารถ และดำเนินการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งในระดับผู้ปฏิบัติงานและผู้บริหาร ควบคู่ไปกับการจัดทำนโยบายและแผน กฎหมาย ระเบียบที่เกี่ยวข้อง รวมทั้งแผนรับมือเหตุการณ์ทางไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนด รวมทั้งจัดหาเครื่องมือ อุปกรณ์ และ

ระบบสนับสนุนต่าง ๆ ในการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) ห้องปฏิบัติการ และศูนย์ปฏิบัติการร่วมทางไซเบอร์ พร้อมทั้งการจัดทำนโยบายและแผน กฎหมายระเบียบ และมาตรฐานที่เกี่ยวข้อง ตลอดจนสนับสนุนงานวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

ในปีที่ 2 มุ่งเน้นการสร้างขีดความสามารถของสำนักงานฯ และระบบบริหารจัดการความมั่นคงปลอดภัย ไซเบอร์ โดย จัดหาเครื่องมือ อุปกรณ์ และระบบสนับสนุนต่าง ๆ ในการจัดตั้งศูนย์ประสานการรักษาความมั่นคง ปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) ห้องปฏิบัติการ และศูนย์ปฏิบัติการร่วมทางไซเบอร์ จัดทำมาตรการและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและ หน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การประเมินความเสี่ยงต่อภัยคุกคามทางไซเบอร์ของ ประเทศ นอกจากนี้ ยังจัดการฝึกซ้อมเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมทั้ง การส่งเสริม สนับสนุน งานวิจัยและพัฒนาที่เกี่ยวข้องด้วย

และปีที่ 3 มุ่งเน้นต่อยอดจากปีที่ 2 โดยการพัฒนาบุคลากรและอุปกรณ์เครื่องมือระบบต่างๆ รวมทั้ง การเผยแพร่สร้างความตระหนักรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง มีการจัดอบรมเพื่อพัฒนาขีดความสามารถผู้ปฏิบัติงานและกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากล ตลอดจนขับเคลื่อนแผนยุทธศาสตร์ด้านความปลอดภัยไซเบอร์ไปสู่การปฏิบัติที่เป็นรูปธรรม

จากแผนจะเห็นว่าสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ต้องดำเนินการ พัฒนาด้านระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ และพัฒนาบุคลากรตั้งแต่ปีแรก รวมถึงพัฒนาการจัดตั้ง ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) ห้องปฏิบัติการ และ ศูนย์ปฏิบัติการร่วมทางไซเบอร์ พร้อมทั้งการจัดทำนโยบายและแผน กฎหมายระเบียบ และมาตรฐานที่เกี่ยวข้อง ตลอดจนสนับสนุนงานวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นภารกิจที่ต้องดำเนินการภายใต้นโยบายรัฐบาลภายใต้เวลาจำกัดอีกด้วย

6.3 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต้องมีผู้บริหารที่มี ความสามารถสูงในการบริหารงานเชิงยุทธศาสตร์

จากความตระหนักในด้านความเสี่ยงบนโลกอินเทอร์เน็ตที่ทวีความรุนแรงมากขึ้นเรื่อยๆ อันเนื่องมาจากภัยคุกคามทางไซเบอร์ที่ซับซ้อนมีการขยายตัวเพิ่มมากขึ้น ซึ่งแน่นอนว่าย่อมส่งผลกระทบต่อ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือ “Critical Information Infrastructure (CII)” ของประเทศ ที่มีการใช้งานคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในกิจการของตนที่เกี่ยวข้องกับการรักษา ความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้าง พื้นฐานอันเป็นประโยชน์สาธารณะ ซึ่งหากถูกโจมตีจากภัยคุกคามทางไซเบอร์แล้ว จะส่งผลกระทบและ ความสูญเสียอย่างร้ายแรงต่อประเทศอย่างมาก ทั้งในด้านเศรษฐกิจ สังคม การดำเนินชีวิตประจำวันของประชาชน ไปจนถึงความมั่นคงของชาติ

ในประเทศไทยมีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศหลายหน่วยงาน ซึ่งหลายหน่วยงานอาจประสบปัญหาในลักษณะการดูแลปัญหา การเฝ้าระวังภัยคุกคาม การปกป้อง การโจมตีทางไซเบอร์ (Cyber Attack) การแก้ไขปัญหาเฉพาะหน้าในการรับมือภัยคุกคาม ตามวิธีและแนวทาง ของตน ยังไม่ได้เป็นมาตรฐานและเป็นไปในทิศทางเดียวกัน ในทำนองเดียวกัน กรณีเกิดการโจมตี Cyber Attack

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศหลายหน่วยงานพร้อมกัน ย่อมจะก่อให้เกิดผลกระทบในวงกว้างต่อทุกภาคส่วน ถือเป็นประเด็นปัญหาที่คาบเกี่ยวข้ามหน่วยงาน (Cross-cutting problem) หากพิจารณาในขอบเขตของแต่ละหน่วยงาน ก็จะประสบปัญหาการทำงานระหว่างกัน เนื่องจากมีรูปแบบการดำเนินงานที่แตกต่างกัน ไม่มีเจ้าภาพในเรื่องการช่วยเหลือหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศในการรับมือภัยคุกคามไซเบอร์ การวิเคราะห์ภัยไซเบอร์ที่มีความยากและซับซ้อนทางเทคนิคในภาพรวมหรือในหลายๆ มิติที่มีผลเชื่อมโยงกัน หรือการสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉิน การประสานความร่วมมือระหว่างภาครัฐและเอกชน ตลอดจนการขาดแคลนบุคลากรที่ปฏิบัติงานที่มีความรู้ ความสามารถเฉพาะทางด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการบ่มเพาะเพื่อสร้างบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ซึ่งมีลักษณะเฉพาะทาง จะต้องใช้ระยะเวลาในการสร้างบุคลากรที่มีศักยภาพ มีความรู้ความสามารถเป็นการเฉพาะ ส่งผลให้เกิดความเสียหายต่อภาคส่วนอื่นๆ หรือขยายในวงกว้างเพิ่มมากขึ้นกระทบต่อเศรษฐกิจ การเงิน การข่าว ความเชื่อมั่นของประชาชนและสังคมของประเทศ นอกจากนี้ ยังส่งผลกระทบต่อการจัดอันดับ Global Cybersecurity Index (CGI) หรือดัชนีความมั่นคงปลอดภัยไซเบอร์โลก โดย ITU ซึ่งจะจัดอันดับจากความรับผิดชอบต่อความมั่นคงปลอดภัยไซเบอร์ในหมู่ประเทศสมาชิก ITU จำนวน 193 ประเทศ โดยพิจารณาจากความพร้อมของแต่ละประเทศ 5 ด้านที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ซึ่งที่ผ่านมา มาตรการเกี่ยวกับองค์กร (Organizational Measures) และความร่วมมือ (Cooperation) ของประเทศไทยยังได้รับคะแนนเล็กน้อย

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งมีผลบังคับใช้เมื่อวันที่ 28 พฤษภาคม 2562 มีวัตถุประสงค์สำคัญประการหนึ่งคือ การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure Protection) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Emergency Readiness) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ (Public-Private Partnership) การประสานความร่วมมือระหว่างหน่วยงานด้านไซเบอร์ทั้งภายในและต่างประเทศ และการสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Capacity Building) เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ที่อาจจะกระทบต่อการดำเนินชีวิตของประชาชนไปจนถึงความมั่นคงของรัฐ เพื่อให้การดำเนินงานของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศสามารถให้บริการประชาชนอย่างต่อเนื่อง

โดยกำหนดสาระสำคัญประการหนึ่งคือ ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ จะต้องปฏิบัติตามประมวลแนวทางปฏิบัติและมาตรฐานขั้นต่ำที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด นอกจากนี้ จะต้องมีการตรวจสอบ การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้แน่ใจว่าระบบสามารถให้บริการได้อย่างต่อเนื่อง ไม่ทำให้ประชาชนเดือดร้อน

อนึ่ง เนื่องจากการรับมือภัยคุกคามด้านไซเบอร์ซึ่งมีการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยี สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งเป็นหน่วยงานที่ถูกกำหนดขึ้นมาภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อทำหน้าที่สำคัญในการรับผิดชอบงานด้านไซเบอร์ในระดับชาติเป็นการเฉพาะ โดยสำนักงานฯ ทำหน้าที่หลายประการ ตั้งแต่ กำหนดนโยบาย กำหนดมาตรฐานขั้นต่ำ ตรวจสอบ ช่วยรับมือภัยคุกคามทางไซเบอร์ที่ถูกแบ่งออกเป็น 3 ระดับ ได้แก่ ระดับแรก คือ “ภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง” เป็นภัยคุกคามทางไซเบอร์ทั่วไปที่ยังไม่รุนแรงมากนัก ระดับที่สอง คือ

“ภัยคุกคามทางไซเบอร์ระดับร้ายแรง” ที่ต้องรับมือ และระดับที่สาม คือ “ภัยคุกคามทางไซเบอร์ระดับวิกฤต” ส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สาธารณูปโภคขั้นพื้นฐาน มีการล่มสลายของระบบเป็นวงกว้าง หรือ มีคนบาดเจ็บล้มตาย เป็นต้น ด้วยเหตุนี้ จึงมีความจำเป็นต้องระดมความร่วมมือจากทุกภาคส่วน ทั้งหน่วยงานภาครัฐ ภาคเอกชน รวมถึงหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งภายในประเทศ และต่างประเทศ เพื่อร่วมกันรับมือภัยคุกคามด้านไซเบอร์ ดังนั้น การพิจารณากำหนดแนวทางหรือวิธีการตรวจสอบ การประเมินความเสี่ยง การรับมือภัยคุกคามทางไซเบอร์ในแต่ละระดับ หรือการปฏิบัติตามแนวทางปฏิบัติที่ได้มาตรฐาน การปฏิบัติตามมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ การเข้าไปช่วยแก้ไข ปัญหาที่เป็น Cross cutting ข้ามหน่วยงาน การดูแลภาครัฐกิจ เอกชน หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ จึงจำเป็นอย่างยิ่งที่ สกมช. จะต้องมีบุคลากรด้านไซเบอร์ที่มีทักษะศักยภาพ เข้าใจบริบทและสมรรถนะที่สูง มีความรู้ความชำนาญทางเทคนิคที่ทันสมัย มีความรู้เท่าทันกับภัยคุกคามทางไซเบอร์ เพื่อเป็นกลไกสำคัญในการขับเคลื่อนองค์กร ตลอดจนการบริหารเครือข่ายของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศทั้ง 7 ด้าน (มาตรา 49 แห่งพระราชบัญญัติฯ) ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณูปโภค และด้านสาธารณสุข ที่มีสาขาทั้งในประเทศและระหว่างประเทศ นอกจากนี้ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ยังต้องทำหน้าที่สำคัญคือการประสานความร่วมมือ รับมือและเผชิญเหตุ ที่เกี่ยวกับภัยคุกคามด้านไซเบอร์ระหว่างประเทศ

จากข้างต้น บทบาท ภารกิจและการทำหน้าที่ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในการเข้าไปช่วยดูแลปัญหา กำหนดกฎเกณฑ์ กรอบมาตรฐานขั้นต่ำ แนวทางปฏิบัติ ตรวจสอบและประเมินการดำเนินงาน การแก้ไขปัญหาเฉพาะหน้า การแก้ไขปัญหาในระยะยาว การผลักดัน สนับสนุนให้หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศเกิดความตระหนักและปฏิบัติตามแนวทางที่กำหนดอย่างสม่ำเสมอและต่อเนื่อง การจัดให้มีการเฝ้าระวังภัยคุกคามและป้องกันการโจมตี เพื่อมุ่งหมายให้หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศสามารถดูแลปกป้องตนเองมีภูมิคุ้มกันภัยไซเบอร์มากขึ้น และสามารถรับมือกับภัยคุกคามไซเบอร์ได้ด้วยตนเอง ถือเป็นงานเร่งด่วนระดับชาติที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในฐานะหน่วยงานที่ดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ทั้งในและนอกประเทศ สมควรจะต้องมีความพร้อมขององค์กรทั้งทางด้านองค์ความรู้ และความเชี่ยวชาญของบุคลากรที่มีทั้งคุณวุฒิ ประสบการณ์และได้รับการเสริมสร้างศักยภาพอย่างต่อเนื่อง เพื่อให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติสามารถพัฒนาทิศทางและวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศในทิศทางที่ถูกต้องเหมาะสม อันจะช่วยเสริมสร้างให้ระบบเศรษฐกิจดิจิทัลของประเทศมีความแข็งแกร่ง สามารถขับเคลื่อนได้อย่างจริงจัง

6.4 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต้องมีการประสานงานกับเครือข่ายทั้งในประเทศหรือระหว่างประเทศ

การประสานความร่วมมือระหว่างภาครัฐ เอกชน ที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ อันได้แก่ (1) ด้านความมั่นคงของรัฐ (2) ด้านบริการภาครัฐที่สำคัญ (3) ด้านการเงินการธนาคาร (4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม (5) ด้านการขนส่งและโลจิสติกส์ (6) ด้านพลังงานและสาธารณูปโภค (7) ด้านสาธารณสุข และ (8) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม

นอกจากนี้ยังมีภารกิจในการพัฒนาผู้มีส่วนได้ส่วนเสีย เช่น พนักงานเจ้าหน้าที่ เจ้าหน้าที่ของหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อประสานงาน เผื่อระวัง รับมือ และแก้ไขภัยคุกคามทาง ไซเบอร์

ดังนั้น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงมีหน้าที่สำคัญ ในการเป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัย ไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ รวมทั้ง การสนับสนุนและให้ ความช่วยเหลือแก่หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

7. สมรรถนะของเลขาธิการคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

7.1 การประเมินค่างาน

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีวัตถุประสงค์สำคัญประการหนึ่งคือ การปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure Protection) การสร้างศักยภาพในการตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Emergency Readiness) การประสานความร่วมมือระหว่างภาครัฐและเอกชนเพื่อความมั่นคงปลอดภัยไซเบอร์ (Public-Private Partnership) การประสานความร่วมมือระหว่างหน่วยงานด้านไซเบอร์ทั้งภายในและต่างประเทศ และการสร้างความตระหนักและรอบรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Capacity Building) เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ที่อาจจะกระทบต่อการดำเนินชีวิตของประชาชนไปจนถึงความมั่นคงของรัฐ เพื่อให้การดำเนินงานของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศสามารถให้บริการประชาชนอย่างต่อเนื่อง โดยกำหนดสาระสำคัญประการหนึ่งคือ ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ จะต้องปฏิบัติตามประมวลแนวทางปฏิบัติและมาตรฐานขั้นต่ำที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กำหนด นอกจากนี้จะต้องมีการตรวจสอบการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้แน่ใจว่าระบบสามารถให้บริการได้อย่างต่อเนื่อง ไม่ทำให้ประชาชนเดือดร้อน

เนื่องจากการรับมือภัยคุกคามด้านไซเบอร์ซึ่งมีการเปลี่ยนแปลงอย่างรวดเร็วของเทคโนโลยี สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งเป็นหน่วยงานที่ถูกกำหนดขึ้นมาภายใต้พระราชบัญญัติฯ เพื่อทำหน้าที่สำคัญในการรับมือกับภัยคุกคามด้านไซเบอร์ในระดับชาติเป็นการเฉพาะ โดยสำนักงานฯ ทำหน้าที่หลายประการ ตั้งแต่ กำหนดนโยบาย กำหนดมาตรฐานขั้นต่ำ ตรวจสอบ ช่วยรับมือภัยคุกคามทางไซเบอร์ที่ถูกแบ่งออกเป็น 3 ระดับ ได้แก่ ระดับแรก คือ “ภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง” เป็นภัยคุกคามทางไซเบอร์ทั่วไปที่ยังไม่รุนแรงมากนัก ระดับที่สอง คือ “ภัยคุกคามทางไซเบอร์ระดับร้ายแรง” ที่ต้องรับมือและระดับที่สาม คือ “ภัยคุกคามทางไซเบอร์ระดับวิกฤต” เป็นภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่นๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ ด้วยเหตุนี้ จึงมีความจำเป็นต้องระดมความร่วมมือจากทุกภาคส่วน ทั้งหน่วยงานภาครัฐ ภาคเอกชน รวมถึงหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งภายในประเทศ และต่างประเทศ เพื่อร่วมกันรับมือภัยคุกคามด้านไซเบอร์ ดังนั้น การพิจารณากำหนดแนวทางหรือวิธีการตรวจสอบ การประเมินความเสี่ยง การรับมือภัยคุกคามทางไซเบอร์ในแต่ละระดับ หรือการปฏิบัติตามแนวทางปฏิบัติที่ได้มาตรฐาน การปฏิบัติตามมาตรการที่ใช้แก้ไขปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ การเข้าไปช่วยแก้ไขปัญหาที่เป็น Cross cutting ข้ามหน่วยงาน การดูแลภาคธุรกิจ เอกชน หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ จึงจำเป็นอย่างยิ่งที่สำนักงานฯ จะต้องมีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ เข้าใจบริบทและสมรรถนะที่สูง มีความรู้ความชำนาญทางเทคนิคที่ทันสมัย มีความรู้เท่าทันกับภัยคุกคามทางไซเบอร์ เพื่อเป็นกลไกสำคัญในการขับเคลื่อนองค์กร ตลอดจน

การบริหารเครือข่ายของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศทั้ง 7 ด้าน (มาตรา 49 แห่งพระราชบัญญัติฯ) ได้แก่ ด้านความมั่นคงของรัฐ ด้านบริการภาครัฐที่สำคัญ ด้านการเงินการธนาคาร ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม ด้านการขนส่งและโลจิสติกส์ ด้านพลังงานและสาธารณสุข และด้านสาธารณสุข และการเป็นศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ รวมทั้ง การสนับสนุนและให้ความช่วยเหลือแก่หน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

ดังนั้น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงมีบทบาท และหน้าที่ในการเข้าไปช่วยดูแลปัญหา กำหนดกฎเกณฑ์ กรอบมาตรฐานขั้นต่ำ แนวทางปฏิบัติ ตรวจสอบและประเมินการดำเนินงาน การแก้ไขปัญหาเฉพาะหน้า การแก้ไขปัญหาในระยะยาว การผลักดัน สนับสนุนให้หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศเกิดความตระหนักและปฏิบัติตามแนวทางที่กำหนดอย่างสม่ำเสมอและต่อเนื่อง การจัดให้มีการเฝ้าระวังภัยคุกคามและปกป้องการโจมตี เพื่อมุ่งหมายให้หน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศสามารถดูแลปกป้องตนเองให้มีภูมิคุ้มกันภัยไซเบอร์มากขึ้น และสามารถรับมือกับภัยคุกคามไซเบอร์ได้ด้วยตนเอง ถือเป็นงานเร่งด่วนระดับชาติที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในฐานะหน่วยงานที่ดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ทั้งในและนอกประเทศ สมควรจะต้องมีความพร้อมขององค์กรทั้งทางด้านองค์ความรู้ และความเชี่ยวชาญของบุคลากรที่มีทั้งคุณวุฒิ ประสบการณ์และได้รับการเสริมสร้างศักยภาพอย่างต่อเนื่อง เพื่อให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติสามารถพัฒนาทิศทางและวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศในทิศทางที่ถูกต้องเหมาะสม อันจะช่วยเสริมสร้างให้ระบบเศรษฐกิจดิจิทัลของประเทศมีความแข็งแกร่ง สามารถขับเคลื่อนได้อย่างจริงจัง

นอกจากนั้น สำนักงานฯ ยังต้องการผู้บริหารที่มีความสามารถสูงในการบริหารงานเชิงยุทธศาสตร์ ใน 3 มิติ ดังนี้

1) มิติด้านความรับผิดชอบในการบริหารงาน

ตามวัตถุประสงค์ ขอบเขตและภารกิจในการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่กำหนดในพระราชบัญญัติพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 นอกจากการรับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ ยังต้องดำเนินการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานต่าง ๆ ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ดำเนินการด้านระบบข่าวกรองทางไซเบอร์ที่เท่าทันกับสถานการณ์ ทั้งอดีต ปัจจุบัน และอนาคต รวมทั้งกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ ในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ พร้อมปรับปรุง กฎหมายให้เท่าทันกับภัยคุกคามทางไซเบอร์ การแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ตลอดจนให้ความช่วยเหลือในการป้องกัน รับมือ และลด

ความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ พร้อมทั้งเสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ และสร้างความตระหนักรู้ด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกันเพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน โดยเป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ ที่ต้องเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน ตลอดจนศึกษาและวิจัยข้อมูลที่สำคัญสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ และจัดให้มีการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์เพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่ที่เกี่ยวข้อง และผลิตนกกกฎหมายให้เข้าใจด้านไซเบอร์

โดยการดำเนินงานดังกล่าวข้างต้นให้บรรลุเป้าหมาย จะต้องใช้เทคนิคหรือเทคโนโลยีที่มีความซับซ้อน เพื่อตอบสนองต่อผู้ให้บริการมีความหลากหลายเพื่อป้องกัน และรับมือต่อภัยคุกคามทางไซเบอร์ ซึ่งจะส่งผลกระทบต่อภาคเศรษฐกิจและสังคมในการยกระดับการรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Information Infrastructure : CII) ให้มีประสิทธิภาพดียิ่งขึ้น พร้อมทั้งมีมาตรการในการป้องกัน รับมือ และลดความเสี่ยงจากการบุกรุกโจมตีไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงของรัฐ เศรษฐกิจ และความสงบเรียบร้อยภายในประเทศที่สอดคล้องกับหลักสากล เพื่อให้ประชาชนไทยเกิดความเชื่อมั่นในการใช้งานเทคโนโลยีดิจิทัล และเกิดความมั่นใจในการทำธุรกรรมออนไลน์และอีคอมเมิร์ซ ซึ่งจะเป็นอีกกลไกหนึ่งในการขับเคลื่อนเศรษฐกิจของประเทศตลอดจนยังช่วยเพิ่มขีดความสามารถทางการแข่งขันในกลุ่มธุรกิจที่เกี่ยวข้องกับโลกดิจิทัล และออนไลน์ ที่จะช่วยป้องกัน และช่วยลดความเสียหายที่จะเกิดขึ้นจากการโจรกรรมได้ รวมทั้งยังช่วยลดปัญหาการขาดแคลนบุคลากรในสาขาที่มีความเกี่ยวข้องกับปัญหาอาชญากรรมบนโลกไซเบอร์ได้โดยตรง ด้วยการพัฒนากำลังคนดิจิทัลด้านไซเบอร์ให้มีความสามารถและเป็นกำลังหลักที่เพียงพอต่อการแข่งขันและพัฒนาประเทศในยุคเศรษฐกิจดิจิทัล เพื่อให้ทุกภาคส่วนของไทยพร้อมรับมือกับภัยคุกคามที่อาจจะเกิดขึ้น

2) มิติด้านประสบการณ์ของผู้อำนวยความสะดวก

จากภารกิจตามกฎหมาย เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงมีความจำเป็นที่ต้องมีความรู้ ความสามารถขั้นสูงในการบริหารจัดการองค์กร ทั้งแบบทั่วไป และแบบเฉพาะทางด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งต้องอาศัยประสบการณ์ ความชำนาญและความเชี่ยวชาญ ความเป็นคนรอบรู้ เป็นที่ยอมรับทั้งในประเทศและต่างประเทศ และที่สำคัญอย่างยิ่งยวดคือต้องเป็นผู้ที่มีความสามารถในการติดต่อสื่อสารที่ดี มีประสิทธิภาพทั้งในประเทศและต่างประเทศ จากภาษาทางเทคนิค วิชาการที่เข้าใจยาก แต่สามารถสื่อสาร แปลความให้ผู้รับสารเข้าถึง เข้าใจได้โดยง่าย มีความเท่าทันต่อการเปลี่ยนแปลงอย่างรวดเร็ว ด้านไซเบอร์ สามารถวางแผนรับมือได้ทั้งเชิงรับและเชิงรุก

3) มิติด้านสถานการณ์

- เป็นการดำเนินงานตามภารกิจและวัตถุประสงค์ของสำนักงานที่ระบุในพระราชบัญญัติฯ เพื่อส่งผลสำเร็จตามนโยบายรัฐบาล ที่ต้องการให้เกิดผลในระยะเวลาอันสั้น รวดเร็ว เร่งด่วนด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งมีความสอดคล้องกับ ยุทธศาสตร์ชาติระยะ 20 ปี (พ.ศ.2560-2579) ในยุทธศาสตร์ที่ 1

ด้านความมั่นคง และยุทธศาสตร์ที่ 2 ด้านการสร้างความสามารถในการแข่งขัน ยุทธศาสตร์แผนพัฒนาฯ ฉบับที่ 12 ด้านความมั่นคง สู่นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2562 - 2565) ด้านการป้องกัน และแก้ไขปัญหาความมั่นคงทางไซเบอร์ รวมถึงนโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจ และสังคมในยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล เป็นต้น นอกจากนี้ขณะที่ประเทศไทย มีการพัฒนาด้านดิจิทัล โดยเฉพาะการทำธุรกรรมผ่านโลกออนไลน์ หรือการดำเนินธุรกรรมทางอิเล็กทรอนิกส์ ภัยคุกคามไซเบอร์จึงเป็นภัยที่ต้องเผชิญอย่างหลีกเลี่ยงไม่ได้การโจมตีระบบ การขโมยข้อมูล การปลอมบัญชี โซเชียลมีเดีย และภัยคุกคามไซเบอร์อื่น ๆ มีปรากฏให้อย่างต่อเนื่อง อาทิ การแพร่ระบาดของ WannaCry ที่เกิดขึ้นทั่วโลก ซึ่งชะลอขีดขวางบริการสารสนเทศของหน่วยงานต่าง ๆ และส่งผลกระทบในการขับเคลื่อน เศรษฐกิจของประเทศล้วนเป็นสถานการณ์เร่งด่วน และสำคัญที่ต้องเตรียมพร้อมเพื่อรับมือต่อความเสียหายที่อาจ เกิดขึ้นและเพื่อให้การดำเนินงานตามภารกิจบรรลุวัตถุประสงค์ตามเป้าหมายของรัฐบาล ผู้ดำรงตำแหน่ง เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จะต้องมีการดำเนินงานตามแผน ขับเคลื่อนในแต่ละช่วงเวลาอย่างต่อเนื่อง เพื่อให้การทำงานมีการสอดประสานและผลักดันได้อย่างเป็นระบบ มีทิศทาง ชัดเจนและเกิดผลสำเร็จอย่างเป็นรูปธรรม

● พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดคุณสมบัติ หน้าที่ และอำนาจ ของเลขาธิการฯ ดังต่อไปนี้

1 คุณสมบัติของเลขาธิการ

- (1) มีสัญชาติไทย
- (2) มีอายุไม่ต่ำกว่าสามสิบห้าปี แต่ไม่เกินหกสิบปี
- (3) เป็นผู้มีความรู้ ความสามารถ และประสบการณ์ในด้านที่เกี่ยวกับการกิจของสำนักงาน และการบริหารจัดการ

2 หน้าที่และอำนาจของเลขาธิการ

พระราชบัญญัติฯ กำหนดให้เลขาธิการภายใต้การควบคุมดูแลของคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัย ไซเบอร์ (กกม.) และ คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) โดย ต้องดำเนินการตามคำสั่งของ กมช. กกม. และ กบส. ภายใต้หน้าที่และอำนาจ ดังต่อไปนี้

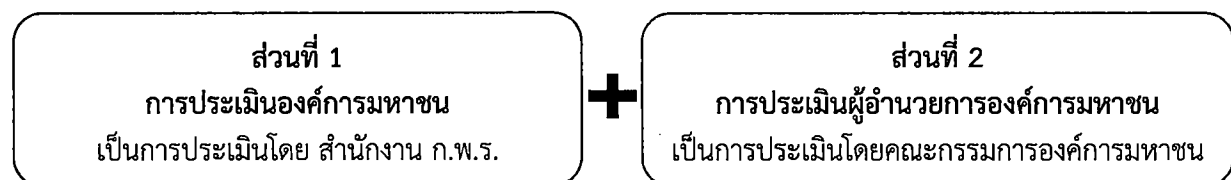
- (1) บริหารงานของสำนักงานให้เกิดผลสัมฤทธิ์ตามภารกิจของสำนักงาน และ ตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคง ปลอดภัยไซเบอร์ นโยบายของคณะรัฐมนตรีและ กมช. และข้อบังคับ นโยบาย มติ และประกาศของ กบส.
- (2) วางระเบียบภายใต้นโยบายของ กมช. และ กกม. โดยไม่ขัดหรือแย้งกับกฎหมายมติของ คณะรัฐมนตรี และข้อบังคับ นโยบาย มติ และประกาศที่ กมช. และ กกม. กำหนด
- (3) เป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน และประเมินผลการปฏิบัติงานของ พนักงานและลูกจ้างของสำนักงานตามข้อบังคับของ กบส. และระเบียบของสำนักงาน
- (4) แต่งตั้งรองเลขาธิการหรือผู้ช่วยเลขาธิการโดยความเห็นชอบของ กมช. เพื่อเป็นผู้ช่วย ปฏิบัติงานของเลขาธิการตามที่เลขาธิการมอบหมาย

(5) บรรจุ แต่งตั้ง เลื่อน ลด ตัดเงินเดือนหรือค่าจ้าง ลงโทษทางวินัยพนักงานและลูกจ้างของสำนักงาน ตลอดจนให้พนักงานและลูกจ้างของสำนักงานออกจากตำแหน่ง ทั้งนี้ ตามข้อบังคับของกบส. และระเบียบของสำนักงาน

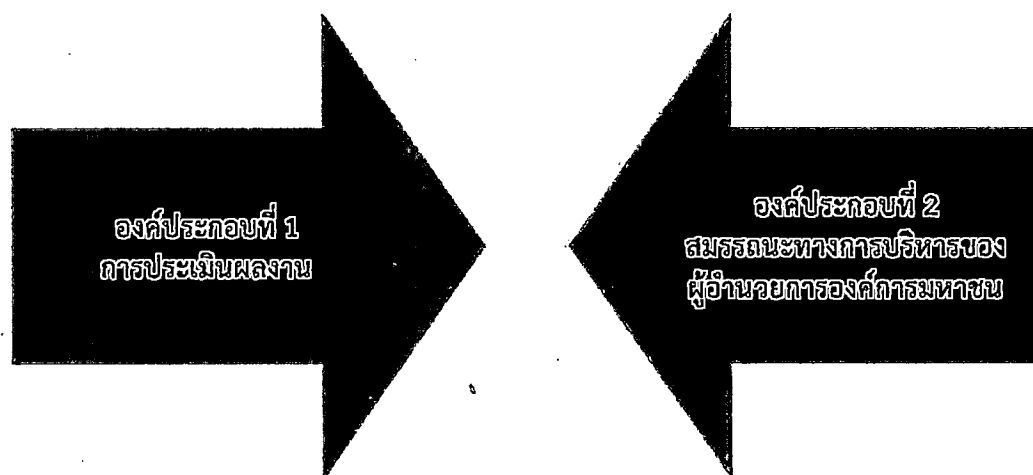
(6) ปฏิบัติการอื่นใดตามข้อบังคับ นโยบาย มติ หรือประกาศของ กบส. หรือ กกม. ในกิจการของสำนักงานที่เกี่ยวกับบุคคลภายนอก ให้เลขาธิการเป็นผู้แทนของสำนักงานภายใต้ขอบเขตที่ได้รับ การแต่งตั้งโดย กกม.

7.2 กรอบการประเมินสมรรถนะของเลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ตามที่กรอบแนวทางการประเมินองค์การมหาชนและผู้อำนวยการองค์การมหาชน ได้กำหนดการประเมินเป็น 2 ส่วน ได้แก่



ในการประเมินสมรรถนะทางการบริหารของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยนำแนวทางมาจากการประเมินผลการปฏิบัติงานของผู้อำนวยการองค์การมหาชน ประจำปี พ.ศ. 2562 ตามหลักเกณฑ์ของสำนักงาน ก.พ.ร. ซึ่งได้กำหนดตัวชี้วัดตามองค์ประกอบในการประเมิน 2 องค์ประกอบ ดังนี้



- 1) ตัวชี้วัดตามสัญญาจ้างผู้อำนวยการองค์การมหาชน
- 2) ผลการประเมินระดับองค์กร
- 3) ตัวชี้วัดตามที่คณะกรรมการมอบหมาย

- 1) ภาวะผู้นำ
- 2) วิสัยทัศน์
- 3) การวางกลยุทธ์
- 4) ศักยภาพเพื่อการปรับเปลี่ยน
- 5) การควบคุมตนเอง
- 6) การสอนงานและการมอบหมายงาน

ข้อมูลประกอบต่อการกำหนดกรอบแนวทางการประเมินผลงาน สรุปได้ ดังนี้

1) ตัวชี้วัดตามสัญญาจ้างเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

การประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ครั้งที่ 3/2563 เมื่อวันที่ 7 ตุลาคม 2563 มีมติเห็นชอบ ตัวชี้วัด เป้าหมายของการปฏิบัติหน้าที่ เลขาธิการ กมช. ดังนี้

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จัดตั้งขึ้นตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งประกาศในราชกิจจานุเบกษา เล่ม 136 ตอนที่ 69 ก เมื่อวันที่ 27 พฤษภาคม 2562 และมีผลใช้บังคับในวันที่ 28 พฤษภาคม 2562 ซึ่งเป็นวันถัดจากวันประกาศในราชกิจจานุเบกษา เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพและเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ

1.1) วัตถุประสงค์

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้ประกาศในราชกิจจานุเบกษา เล่ม 136 ตอนที่ 69 ก เมื่อวันที่ 27 พฤษภาคม 2562 และมีผลใช้บังคับในวันที่ 28 พฤษภาคม 2562 ซึ่งเป็นวันถัดจากวันประกาศในราชกิจจานุเบกษา ซึ่งตามพระราชบัญญัตินี้กำหนดให้เลขาธิการรับผิดชอบการปฏิบัติงานของสำนักงาน เป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน รวมทั้งต้องดำเนินการภายใต้การควบคุมดูแลและคำสั่งของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) และคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) ภายใต้หน้าที่และอำนาจ ดังต่อไปนี้

(1) บริหารงานของสำนักงานให้เกิดผลสัมฤทธิ์ตามภารกิจของสำนักงานและตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบายของคณะรัฐมนตรีและคณะกรรมการ และข้อบังคับ นโยบาย มติ และประกาศของ กบส.

(2) วางระเบียบภายใต้นโยบายของคณะกรรมการและ กกม. โดยไม่ขัดหรือแย้งกับกฎหมาย มติของคณะรัฐมนตรี และข้อบังคับ นโยบาย มติ และประกาศที่คณะกรรมการและ กกม. กำหนด

(3) เป็นผู้บังคับบัญชาพนักงานและลูกจ้างของสำนักงาน และประเมินผลการปฏิบัติงานของพนักงานและลูกจ้างของสำนักงานตามข้อบังคับของ กบส. และระเบียบของสำนักงาน

(4) แต่งตั้งรองเลขาธิการหรือผู้ช่วยเลขาธิการโดยความเห็นชอบของคณะกรรมการ เพื่อเป็นผู้ช่วยปฏิบัติงานของเลขาธิการตามที่เลขาธิการมอบหมาย

(5) บรรจุ แต่งตั้ง เลื่อน ลด ตัดเงินเดือนหรือค่าจ้าง ลงโทษทางวินัยพนักงานและลูกจ้างของสำนักงาน ตลอดจนให้พนักงานและลูกจ้างของสำนักงานออกจากตำแหน่ง ทั้งนี้ ตามข้อบังคับของ กบส. และระเบียบของสำนักงาน

(6) ปฏิบัติการอื่นใดตามข้อบังคับ นโยบาย มติ หรือประกาศของ กบส. หรือ กกม. รวมทั้งต้องปฏิบัติงานของสำนักงานตามที่พระราชบัญญัตินี้กำหนดไว้

1.2) เป้าหมาย

(1) การจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้มีความพร้อมสามารถดำเนินงานบรรลุวัตถุประสงค์และเป้าหมายที่กำหนด ภายในปี 2565

(2) การดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นไปตามวัตถุประสงค์ที่กำหนดไว้ในกฎหมาย โดยสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561-2580) นโยบาย และแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ พ.ศ. 2562-2565

(3) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นศูนย์กลาง ประสานความร่วมมือระหว่างหน่วยงานเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและ หน่วยงานเอกชน ทั้งในประเทศและต่างประเทศ

(4) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นองค์กรของรัฐ ที่มีระบบการบริหารจัดการที่มีธรรมาภิบาล มีประสิทธิภาพและมุ่งเน้นประโยชน์ส่วนรวมเป็นสำคัญ

1.3) ตัวชี้วัด

(1) มีการจัดตั้งและบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้มีทรัพยากรบุคคล ระบบข้อมูลและองค์ความรู้เพื่อรองรับการปฏิบัติงาน รวมทั้งพัฒนาระบบการบริหารจัดการ สารสนเทศและดิจิทัล และการสื่อสารประชาสัมพันธ์ให้เกิดการรับรู้แก่ผู้ที่เกี่ยวข้อง ภายในปี 2565

(2) การจัดทำและดำเนินการตามนโยบาย แผน และยุทธศาสตร์เกี่ยวกับการรักษา ความมั่นคงปลอดภัยไซเบอร์

(3) การบริหารจัดการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้ เป็นไปตามวัตถุประสงค์ของกฎหมาย นโยบาย มติของ กมช. กกม. และ กบส. และกฎหมายที่เกี่ยวข้อง ภายในปี 2565

(4) แนวทางในการส่งเสริมและผลักดันให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ มีความพร้อมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

(5) แนวทางและมาตรการในการพัฒนาสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย ไซเบอร์แห่งชาติให้มีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์

(6) มีกฎหมายลำดับรองที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องและ เป็นไปตามมาตรฐานสากล

(7) มีรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบ อย่างมีนัยสำคัญต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

1.4) ผลผลิต

(1) มีนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์และแผนปฏิบัติการ เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการพิจารณาอนุมัติจากคณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ

(2) มีแนวทางในการส่งเสริมและผลักดันให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมี ความพร้อมในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่ได้รับการพิจารณาอนุมัติจาก คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

(3) มีแนวทางและมาตรการในการพัฒนาสำนักงานคณะกรรมการการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติให้มีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่ได้รับการพิจารณาอนุมัติจาก คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

(4) มีกฎหมายลำดับรองที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องและเป็นไปตามมาตรฐานสากล อย่างน้อย 5 ฉบับตามความสำคัญเร่งด่วน

(5) มีรายงานการวิเคราะห์สภาพปัญหาและสถานการณ์ อุปสรรค และความสำเร็จ ในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์เป็นรายปีที่เสนอคณะรัฐมนตรี

2) กรอบการประเมินผลองค์การมหาชน

สำนักงาน ก.พ.ร. ได้แจ้งกรอบการประเมินผลองค์การมหาชน ประจำปีงบประมาณ พ.ศ. 2564 ดังนี้

กรอบการประเมินผลองค์การมหาชน ประจำปีงบประมาณ พ.ศ. 2564			
1. องค์ประกอบการประเมินผลการปฏิบัติงาน			
Performance Perspective	องค์ประกอบ/ตัวชี้วัดและประเด็นการประเมิน	น้ำหนัก	
	องค์ประกอบที่ 1 ประสิทธิภาพการดำเนินงาน	40	
	1.1 ตัวชี้วัดที่สอดคล้องกับการติดตามวัตถุประสงค์การจัดตั้งที่แสดงให้เห็นการเชื่อมโยงจากยุทธศาสตร์ชาติ นโยบาย และแผนระดับชาติ	30	
	1.2 ตัวชี้วัดที่สอดคล้องกับประเด็นการปฏิรูปประเทศของกระทรวงที่เกี่ยวข้องนโยบายสำคัญหรือเร่งด่วนของรัฐบาล (องค์การมหาชนเสนอ : 1 องค์การมหาชน 1 ประเด็นการปฏิรูปประเทศ อย่างน้อย 1 ตัวชี้วัด และอาจเสนอตัวชี้วัดที่สอดคล้องกับนโยบายสำคัญหรือเร่งด่วนของรัฐบาลเพิ่มเติมได้อีก 1 ตัวชี้วัด)	10	
	องค์ประกอบที่ 2 ประสิทธิภาพและความคุ้มค่าในการดำเนินงาน	30	
	2.1 ตัวชี้วัดที่แสดงถึงประสิทธิภาพในการบริหารงาน/ความคุ้มค่าในการดำเนินงาน	25	
	2.2 ร้อยละค่าใช้จ่ายด้านบุคลากรขององค์การมหาชน	5	
Potential Perspective	องค์ประกอบที่ 3 ศักยภาพขององค์การมหาชน	20	
	3.1 ผลการพัฒนาศักยภาพองค์การสู่การเป็นระบบราชการ 4.0	10	
	3.1.1 การพัฒนาองค์การสู่ดิจิทัล (เลือก 1 จาก 2 ตัวชี้วัดย่อยต่อไปนี้) 1) การพัฒนาระบบบัญชีข้อมูล (Data Catalog) เพื่อนำไปใช้สู่การเปิดเผยข้อมูลภาครัฐ (Open Data) 2) การให้บริการผ่านระบบอิเล็กทรอนิกส์ (e-Service) เงื่อนไข : เป้าหมายขั้นต่ำให้รวมถึงการเปิดเผยข้อมูลผ่าน Web Portal และ Website ขององค์การมหาชนอย่างครบถ้วน และเป็นปัจจุบัน		
	3.1.2 การประเมินสถานะของหน่วยงานภาครัฐในการเป็นระบบราชการ 4.0 (PMQA 4.0)		10
	องค์ประกอบที่ 4 การควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน	10	
	4.1 ร้อยละความสำเร็จของการพัฒนาด้านการควบคุมดูแลกิจการของคณะกรรมการองค์การมหาชน	10	
2. ตัวชี้วัดประกอบการประเมิน (รายงานผลคะแนนพร้อมกับผลประเมินองค์การมหาชนและไม่นำมาคำนวณคะแนน)			
 การประเมินคุณธรรมและความโปร่งใสในการดำเนินงานของหน่วยงานภาครัฐ (สำนักงาน ป.ป.ช.)			
3. ตัวชี้วัด monitor (ไม่นำมาคำนวณคะแนน)			
 ตัวชี้วัดผลกระทบ (Impact) เพื่อติดตามผลสำเร็จเป็นรายปี (monitoring KPI) โดยให้องค์การมหาชนรายงานผลตามตัวชี้วัดมายังสำนักงาน ก.พ.ร. แต่ไม่นำมาคำนวณคะแนน			
กรณี PO : นำผลการประเมินสะสมไปใช้ประเมินความคุ้มค่าในการจัดตั้งฯ ทุก 5 ปี ในวาระแรก 3 ปี (พ.ศ. 2563 – 2565) และประกอบการรายงาน ครม. กรณี PA : นำผลการประเมินไปใช้ประกอบการรายงาน ครม.			

การกำหนดกรอบการประเมินสมรรถนะทางการบริหารของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

จากข้อมูลข้างต้น ในกรณีนี้ จึงได้กำหนดการประเมินสมรรถนะของเลขาธิการสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติ โดยมีรายละเอียด ดังนี้

1. หลักเกณฑ์การกำหนดสมรรถนะของเลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ประเภทสมรรถนะ	องค์ประกอบการประเมิน
1. ผลงานของผู้อำนวยการองค์การมหาชน (Performance)	1. สัญญาจ้างเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
	2. ผลการประเมินองค์กร
	3. งานอื่นๆ ที่คณะกรรมการมอบหมาย
2. สมรรถนะทางการบริหารของผู้อำนวยการองค์การมหาชน (Competency)	1. ภาวะผู้นำ
	2. วิสัยทัศน์
	3. การวางกลยุทธ์ขององค์การมหาชน
	4. ศักยภาพเพื่อนำการปรับเปลี่ยน
	5. การควบคุมตนเอง
	6. การสอนงานและการมอบหมายงาน

2. เกณฑ์การประเมิน

2.1 การแปลผลการประเมิน

แนวทางการประเมินผลการปฏิบัติงานของผู้อำนวยการองค์การมหาชน ประจำปี พ.ศ. 2562 ตามหลักเกณฑ์ของสำนักงาน ก.พ.ร. ได้แบ่งเป็น 3 ระดับ คือ ระดับตัวชี้วัด ระดับองค์ประกอบ และระดับภาพรวม ดังนี้

1) ระดับตัวชี้วัด

ประเมินผลการดำเนินงานในแต่ละตัวชี้วัดภายในแต่ละองค์ประกอบ โดยเปรียบเทียบผลการดำเนินงานจริงกับค่าเป้าหมายที่ระบุในแต่ละรอบการประเมิน ดังนี้

☒	ผ่าน หมายถึง ผลการดำเนินงานเป็นไปตามเป้าหมาย หรือสูงกว่าเป้าหมายที่ตั้งไว้
☐	ไม่ผ่าน หมายถึง ผลการดำเนินงานต่ำกว่าเป้าหมายที่ตั้งไว้

2) ระดับองค์ประกอบ

ประเมินผลการดำเนินงานในระดับองค์ประกอบ ภายหลังจากการได้ผลการประเมินระดับตัวชี้วัดแล้ว โดยพิจารณาจากร้อยละตัวชี้วัดที่ดำเนินการบรรลุเป้าหมายต่อตัวชี้วัดทั้งหมด ในองค์ประกอบนั้นๆ ดังนี้

☐	ต่ำกว่าเป้าหมาย หมายถึง ร้อยละของตัวชี้วัดที่ดำเนินการบรรลุเป้าหมายต่อตัวชี้วัดทั้งหมด ต่ำกว่าร้อยละ 50
☒	เป็นไปตามเป้าหมาย หมายถึง ร้อยละของตัวชี้วัดที่ดำเนินการบรรลุเป้าหมายต่อตัวชี้วัดทั้งหมด ระหว่างร้อยละ 50-67
☒	สูงกว่าเป้าหมาย หมายถึง ร้อยละของตัวชี้วัดที่ดำเนินการบรรลุเป้าหมายต่อตัวชี้วัดทั้งหมด สูงกว่าร้อยละ 67

3) ระดับภาพรวม

ประเมินผลการดำเนินงานในระดับองค์ประกอบ ภายหลังจากการได้ผลการประเมินระดับตัวชี้วัดแล้ว โดยพิจารณาจากร้อยละตัวชี้วัดที่ดำเนินการบรรลุเป้าหมายต่อตัวชี้วัดทั้งหมด ในองค์ประกอบนั้นๆ ดังนี้

ระดับ		ความหมาย
คุณภาพ  (สีเขียว)	ระดับ 1	- องค์การมหาชนมีการกำหนดตัวชี้วัดประเภทผลลัพธ์ ในองค์ประกอบ Function/ Agenda/ Area ร้อยละ 80 ขึ้นไป - มีผลการประเมินสูงกว่าเป้าหมายทุกองค์ประกอบ - มีตัวชี้วัดที่ผ่านการประเมินร้อยละ 100
	ระดับ 2	- องค์การมหาชนมีการกำหนดตัวชี้วัดประเภทผลลัพธ์ ในองค์ประกอบ Function/ Agenda/ Area น้อยกว่าร้อยละ 80 - มีผลการประเมินสูงกว่าเป้าหมายทุกองค์ประกอบ - มีตัวชี้วัดที่ผ่านการประเมินร้อยละ 100
	ระดับ 3	- องค์การมหาชนมีการกำหนดตัวชี้วัดประเภทผลลัพธ์ ในองค์ประกอบ Function/ Agenda/ Area น้อยกว่าร้อยละ 80 - มีผลการประเมินสูงกว่าเป้าหมายทุกองค์ประกอบ - มีตัวชี้วัดที่ผ่านการประเมินน้อยกว่าร้อยละ 100
มาตรฐาน  (สีเหลือง)	ระดับ 4	- องค์การมหาชนมีการกำหนดตัวชี้วัดประเภทผลลัพธ์ ในองค์ประกอบ Function/ Agenda/ Area น้อยกว่าร้อยละ 80 - มีผลการประเมินสูงกว่าเป้าหมายบางองค์ประกอบ แต่ไม่มีองค์ประกอบใดต่ำกว่าเป้าหมาย - มีตัวชี้วัดที่ผ่านการประเมินน้อยกว่าร้อยละ 100
ต้องปรับปรุง  (สีแดง)	ระดับ 5	- องค์การมหาชนมีการกำหนดตัวชี้วัดประเภทผลลัพธ์ ในองค์ประกอบ Function/ Agenda/ Area น้อยกว่าร้อยละ 80 - มีผลการประเมินสูงกว่าเป้าหมายบางองค์ประกอบ และมีองค์ประกอบใดองค์ประกอบหนึ่งต่ำกว่าเป้าหมาย - มีตัวชี้วัดที่ผ่านการประเมินน้อยกว่าร้อยละ 100

2.2 เกณฑ์การประเมินสมรรถนะทางการบริหารของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เกณฑ์การประเมินสมรรถนะทางการบริหารของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยการนำแนวทางการประเมินผลการปฏิบัติงานของผู้อำนวยการองค์การมหาชน ประจำปี พ.ศ. 2562 ตามหลักเกณฑ์ของสำนักงาน ก.พ.ร. เกณฑ์การประเมินสมรรถนะทางการบริหารของผู้อำนวยการองค์การมหาชน มีรายละเอียด ดังนี้

1) ภาวะผู้นำ (Leadership) หมายถึง ความสามารถหรือความตั้งใจที่จะรับบทในการเป็นผู้นำขององค์กรมหาชน กำหนดทิศทาง เป้าหมาย วิธีการทำงาน ให้ผู้ใต้บังคับบัญชาได้อย่างราบรื่น เต็มประสิทธิภาพและบรรลุวัตถุประสงค์ขององค์กรมหาชน

ระดับของสมรรถนะ		พฤติกรรมบ่งชี้
ระดับ 1 ต่ำกว่าเป้าหมาย	- ดำเนินการประชุมได้ดีและคอยแจ้งข่าวสารความเป็นไปโดยตลอด - เป็นผู้นำในการทำงานของกลุ่มและใช้อำนาจอย่างยุติธรรม	- ดำเนินการประชุมให้เป็นไปตามระเบียบวาระวัตถุประสงค์และเวลา ตลอดจนมอบหมายงานให้แก่บุคคลในกลุ่มได้ - แจ้งข่าวสารให้ผู้ที่จะได้รับผลกระทบจากการตัดสินใจรับทราบอยู่เสมอ แม้ไม่ได้ถูกกำหนดให้ต้องกระทำ - อธิบายเหตุผลในการตัดสินใจให้ผู้ที่เกี่ยวข้องทราบ - ส่งเสริมและกระทำการเพื่อให้กลุ่มปฏิบัติหน้าที่ได้อย่างเต็มประสิทธิภาพ - กำหนดเป้าหมาย ทิศทางที่ชัดเจน จัดกลุ่มงาน และเลือกคนให้เหมาะกับงาน หรือกำหนดวิธีการที่จะทำให้กลุ่มทำงานได้ดีขึ้น - รับฟังความคิดเห็นของผู้อื่น สร้างขวัญกำลังใจในการปฏิบัติงานปฏิบัติต่อสมาชิกในทีมด้วยความยุติธรรม
ระดับ 2 เป็นไปตามเป้าหมาย	- แสดงสมรรถนะระดับ 1 และ - ให้การดูแลและช่วยเหลือทีมงาน - ประพฤติสมกับเป็นผู้นำ	- เป็นที่ปรึกษาและช่วยเหลือทีมงาน - ปกป้องทีมงานและชื่อเสียงขององค์กร - จัดหาบุคลากร ทรัพยากรหรือข้อมูลที่สำคัญมาให้ทีมงาน - กำหนดธรรมเนียมปฏิบัติประจำกลุ่มและประพฤติตนอยู่ในกรอบของธรรมเนียมปฏิบัตินั้น - ประพฤติปฏิบัติตนอย่างเป็นแบบอย่างที่ดี - ยึดหลักธรรมาภิบาลในการปกครองผู้ใต้บังคับบัญชา
ระดับ 3 สูงกว่าเป้าหมาย	- แสดงสมรรถนะระดับ 2 และ - นำทีมงานให้ก้าวไปสู่พันธกิจระยะยาวขององค์กร	- สามารถรวมใจคนและสร้างแรงบันดาลใจให้ทีมงานเกิดความมั่นใจในการปฏิบัติภารกิจให้สำเร็จลุล่วง - เล็งเห็นการเปลี่ยนแปลงในอนาคตและมีวิสัยทัศน์ในการสร้างกลยุทธ์เพื่อรับมือกับการเปลี่ยนแปลงนั้น

2) **วิสัยทัศน์ (Visioning)** หมายถึง ความสามารถในการกำหนดทิศทาง การกิจ และเป้าหมายการทำงานที่ชัดเจนและความสามารถในการสร้างความร่วมแรงร่วมใจเพื่อให้ภารกิจบรรลุวัตถุประสงค์

ระดับของสมรรถนะ		พฤติกรรมบ่งชี้
ระดับ 1 ต่ำกว่าเป้าหมาย	- รู้และเข้าใจวิสัยทัศน์ขององค์กร - ช่วยทำให้ผู้อื่นรู้และเข้าใจวิสัยทัศน์ขององค์กร	- รู้ เข้าใจ และสามารถอธิบายให้ผู้อื่นเข้าใจได้ว่างานที่ทำอยู่นั้นเกี่ยวข้องหรือตอบสนองต่อวิสัยทัศน์ขององค์การมาหาอย่างไร - อธิบายให้ผู้อื่นรู้และเข้าใจวิสัยทัศน์และเป้าหมายการทำงานของหน่วยงานภายใต้ภาพรวมขององค์การมาหาขึ้นได้ - แลกเปลี่ยนข้อมูลรวมถึงรับฟังความคิดเห็นของผู้อื่นเพื่อประกอบการกำหนดวิสัยทัศน์
ระดับ 2 เป็นไปตามเป้าหมาย	- แสดงสมรรถนะระดับ 1 และ - สร้างแรงจูงใจให้ผู้อื่นเต็มใจที่จะปฏิบัติตามวิสัยทัศน์ - กำหนดนโยบายให้สอดคล้องกับวิสัยทัศน์ของหน่วยงาน	- โน้มน้าวให้สมาชิกในทีมเกิดความเต็มใจและกระตือรือร้นที่จะปฏิบัติหน้าที่เพื่อตอบสนองต่อวิสัยทัศน์ - ให้คำปรึกษาแนะนำแก่สมาชิกในทีมถึงแนวทางในการทำงานโดยยึดถือวิสัยทัศน์และเป้าหมายขององค์กรเป็นสำคัญ - ริเริ่มและกำหนดนโยบายใหม่ ๆ เพื่อตอบสนองต่อการนำวิสัยทัศน์ไปสู่ความสำเร็จ
ระดับ 3 สูงกว่าเป้าหมาย	- แสดงสมรรถนะระดับ 2 และ - กำหนดนโยบายให้สอดคล้องกับวิสัยทัศน์ระดับประเทศ	- กำหนดวิสัยทัศน์ เป้าหมาย และทิศทางในการปฏิบัติหน้าที่ขององค์การมาหาเพื่อบรรลุวิสัยทัศน์ซึ่งสอดคล้องกับวิสัยทัศน์ระดับประเทศ - คาดการณ์ได้ว่าประเทศจะได้รับผลกระทบอย่างไรจากการเปลี่ยนแปลงทั้งภายในและภายนอก

3) **การวางกลยุทธ์ขององค์การมาหา (Strategic Orientation)** หมายถึง ความเข้าใจวิสัยทัศน์และนโยบายภาครัฐและสามารถนำมาประยุกต์ใช้ในการกำหนดกลยุทธ์ขององค์การมาหา

ระดับของสมรรถนะ		พฤติกรรมบ่งชี้
ระดับ 1 ต่ำกว่าเป้าหมาย	- รู้และเข้าใจนโยบายรัฐบาลว่ามีความเกี่ยวข้องกับหน้าที่ความรับผิดชอบขององค์การมาหาอย่างไร - นำประสบการณ์มาประยุกต์ใช้ในการกำหนดกลยุทธ์ได้	- เข้าใจนโยบายรัฐบาล รวมทั้ง กลยุทธ์ของภาครัฐว่าสัมพันธ์เชื่อมโยงกับภารกิจขององค์การมาหาที่ตนดูแลรับผิดชอบอย่างไร - สามารถวิเคราะห์ปัญหาอุปสรรคหรือโอกาสขององค์การมาหาขึ้นได้

ระดับของสมรรถนะ		พฤติกรรมบ่งชี้
		• ประยุกต์ใช้ประสบการณ์ในการกำหนดกลยุทธ์ขององค์การมหาชนให้สอดคล้องกับยุทธศาสตร์ภาครัฐได้ • ใช้ความรู้ความเข้าใจในระบบราชการมาปรับกลยุทธ์ให้เหมาะสมกับสถานการณ์ที่เปลี่ยนแปลงได้
ระดับ 2 เป็นไปตามเป้าหมาย	• แสดงสมรรถนะระดับ 1 และ • นำทฤษฎีหรือแนวคิดซับซ้อนมากำหนดกลยุทธ์ • กำหนดกลยุทธ์ที่สอดคล้องกับสถานการณ์ต่างๆ ที่เกิดขึ้น	• ประยุกต์ใช้ทฤษฎีหรือแนวคิดซับซ้อน ในการคิดและพัฒนาเป้าหมายหรือกลยุทธ์ขององค์การมหาชน • ประยุกต์แนวทางปฏิบัติที่ประสบความสำเร็จ (Best Practice) หรือผลการวิจัยต่าง ๆ มากำหนดแผนงานเชิงกลยุทธ์ในองค์การมหาชน • ประเมินและสังเคราะห์สถานการณ์ประเด็นหรือปัญหาทางเศรษฐกิจสังคมการเมืองภายในประเทศหรือของโลกโดยมองภาพรวมในลักษณะองค์รวมเพื่อใช้ในการกำหนดกลยุทธ์ขององค์การมหาชน
ระดับ 3 สูงกว่าเป้าหมาย	• แสดงสมรรถนะระดับ 2 และ • บูรณาการองค์ความรู้ใหม่มาใช้ในการกำหนดกลยุทธ์ขององค์การมหาชน	• ริเริ่ม สร้างสรรค์และบูรณาการองค์ความรู้ใหม่ในการกำหนดกลยุทธ์ขององค์การมหาชนโดยพิจารณาจากบริบทในภาพรวม • ปรับเปลี่ยนทิศทางของกลยุทธ์ในการพัฒนาประเทศอย่างต่อเนื่อง

4) ศักยภาพเพื่อนำการปรับเปลี่ยน (Change Leadership) หมายถึง ความสามารถในการกระตุ้นหรือผลักดันองค์การมหาชนไปสู่การปรับเปลี่ยนที่เป็นประโยชน์ รวมถึงการสื่อสารให้ผู้อื่นรับรู้ เข้าใจและดำเนินการให้การปรับเปลี่ยนเกิดขึ้นจริง

ระดับของสมรรถนะ		พฤติกรรมบ่งชี้
ระดับ 1 ต่ำกว่าเป้าหมาย	• เห็นความจำเป็นของการปรับเปลี่ยน • สามารถทำให้ผู้อื่นเข้าใจการปรับเปลี่ยนที่จะเกิดขึ้น	• เห็นความจำเป็นของการปรับเปลี่ยนและปรับพฤติกรรมหรือแผนการทำงานให้สอดคล้องกับการเปลี่ยนแปลงนั้น • เข้าใจและยอมรับถึงความจำเป็นของการปรับเปลี่ยนและเรียนรู้เพื่อให้สามารถปรับตัวรับการเปลี่ยนแปลงนั้นได้ • ช่วยเหลือให้ผู้อื่นเข้าใจถึงความจำเป็นและประโยชน์ของการเปลี่ยนแปลงนั้น • สนับสนุนความพยายามในการปรับเปลี่ยน

ระดับของสมรรถนะ		พฤติกรรมบ่งชี้
		องค์กร พร้อมทั้งเสนอแนะวิธีการและมีส่วนร่วมในการปรับเปลี่ยนดังกล่าว
ระดับ 2 เป็นไปตามเป้าหมาย	● แสดงสมรรถนะระดับ 1 และ ● นำทฤษฎีหรือแนวคิดซับซ้อนมากำหนดกลยุทธ์ ● วางแผนงานที่ดีเพื่อรับการปรับเปลี่ยนในองค์กร	● กระตุ้นและสร้างแรงจูงใจให้ผู้อื่นเห็นความสำคัญของการปรับเปลี่ยนเพื่อให้เกิดความร่วมมือร่วมใจ ● เปรียบเทียบให้เห็นว่าสิ่งที่ปฏิบัติอยู่ในปัจจุบันกับสิ่งที่เปลี่ยนแปลงไปนั้นแตกต่างกันในสาระสำคัญอย่างไร ● สร้างความเข้าใจให้เกิดขึ้นแก่ผู้ที่ยังไม่ยอมรับการเปลี่ยนแปลงนั้น ● วางแผนอย่างเป็นระบบและชี้ให้เห็นประโยชน์ของการปรับเปลี่ยน ● เตรียมแผนและติดตามการบริหารการเปลี่ยนแปลงอย่างสม่ำเสมอ
ระดับ 3 สูงกว่าเป้าหมาย	● แสดงสมรรถนะระดับ 2 และ ● ผลักดันให้เกิดการปรับเปลี่ยนอย่างมีประสิทธิภาพ	● ผลักดันให้การปรับเปลี่ยนสามารถดำเนินไปได้ อย่างราบรื่นและประสบความสำเร็จ ● สร้างขวัญ กำลังใจ และความเชื่อมั่นในการขับเคลื่อนให้เกิดการปรับเปลี่ยนอย่างมีประสิทธิภาพ

5) การควบคุมตนเอง (Self Control) หมายถึง ความสามารถในการควบคุมอารมณ์และพฤติกรรมในสถานการณ์ที่อาจถูกยั่วยุ หรือเผชิญหน้ากับความไม่เป็นมิตร หรือต้องทำงานภายใต้สภาวะกดดัน รวมถึงความอดทนอดกลั้นเมื่ออยู่ในสถานการณ์ที่ก่อความเครียดอย่างต่อเนื่อง

ระดับของสมรรถนะ		พฤติกรรมบ่งชี้
ระดับ 1 ต่ำกว่าเป้าหมาย	● ไม่แสดงพฤติกรรมที่ไม่เหมาะสม ● ควบคุมอารมณ์ในแต่ละสถานการณ์ได้เป็นอย่างดี	● ไม่แสดงพฤติกรรมที่ไม่สุภาพหรือไม่เหมาะสมในทุกสถานการณ์ ● รู้เท่าทันอารมณ์ของตนเองและควบคุมได้อย่างเหมาะสม โดยอาจหลีกเลี่ยงจากสถานการณ์เสี่ยงต่อการเกิดความรุนแรงขึ้นหรืออาจเปลี่ยนหัวข้อสนทนาหรือหยุดพักชั่วคราวเพื่อสงบสติอารมณ์
ระดับ 2 เป็นไปตามเป้าหมาย	● แสดงสมรรถนะระดับ 1 และ ● สามารถใช้ถ้อยทีวาทจาหรือปฏิบัติงานต่อไปได้อย่างสงบแม้จะอยู่ในภาวะที่ถูกยั่วยุ ● จัดการความเครียดได้อย่างมีประสิทธิภาพ	● รู้สึกได้ถึงความรุนแรงทางอารมณ์ในระหว่างสนทนาหรือการปฏิบัติงาน เช่น ความโกรธ ความผิดหวัง หรือความกดดันแต่ไม่แสดงออกแม้ถูกยั่วยุ โดยยังคงสามารถปฏิบัติงานต่อไปได้อย่างสงบ ● สามารถเลือกใช้วิธีการแสดงออกที่เหมาะสมเพื่อ

ระดับของสมรรถนะ		พฤติกรรมบ่งชี้
	ประสิทธิภาพ	ไม่ให้เกิดผลในเชิงลบทั้งต่อตนเองและผู้อื่น • สามารถจัดการกับความเครียดหรือผลที่อาจเกิดขึ้นจากสภาวะกดดันทางอารมณ์ได้อย่างมีประสิทธิภาพ • ประยุกต์ใช้วิธีการเฉพาะตนหรือวางแผนล่วงหน้าเพื่อจัดการกับความเครียดและความกดดันทางอารมณ์ที่คาดการณ์ได้ว่าจะเกิดขึ้น • บริหารจัดการอารมณ์ของตนได้อย่างมีประสิทธิภาพเพื่อลดความเครียดของตนเองหรือเพื่อนร่วมงาน
ระดับ 3 สูงกว่าเป้าหมาย	• แสดงสมรรถนะระดับ 2 และ • เอาชนะอารมณ์ด้วยความเข้าใจ	• ระบุความรุนแรงด้วยการพยายามทำความเข้าใจและแก้ไขที่ต้นเหตุของปัญหารวมทั้งบริบทและปัจจัยแวดล้อมต่างๆ • ในสถานการณ์ที่ตึงเครียดมากก็ยังสามารถควบคุมอารมณ์ของตนเองได้รวมถึงทำให้คนอื่นๆ มีอารมณ์ที่สงบลงได้

6) การสอนงานและการมอบหมายงาน (Coaching and Empowering Others) หมายถึง ความตั้งใจที่จะส่งเสริมการเรียนรู้หรือการพัฒนาผู้อื่นในระยะยาวจนถึงระดับที่เชื่อมั่นว่าจะสามารถมอบหมายหน้าที่ความรับผิดชอบให้ผู้นั้นมีอิสระที่จะตัดสินใจในการปฏิบัติหน้าที่ของตนได้

ระดับของสมรรถนะ		พฤติกรรมบ่งชี้
ระดับ 1 ต่ำกว่าเป้าหมาย	• สอนงานหรือให้คำแนะนำเกี่ยวกับวิธีปฏิบัติงาน • ตั้งใจพัฒนาผู้ใต้บังคับบัญชาให้มีศักยภาพ	• สอนงานด้วยการให้คำแนะนำอย่างละเอียด หรือด้วยการสาธิตวิธีปฏิบัติงาน • ชี้แนะแหล่งข้อมูลหรือแหล่งทรัพยากรอื่นๆ เพื่อใช้ในการพัฒนาการปฏิบัติงาน • สามารถให้คำปรึกษาชี้แนะแนวทางในการพัฒนาหรือส่งเสริมข้อดีและปรับปรุงข้อด้อยให้ลดลง • ให้โอกาสผู้ใต้บังคับบัญชาได้แสดงศักยภาพเพื่อสร้างความมั่นใจในการปฏิบัติงาน
ระดับ 2 เป็นไปตามเป้าหมาย	• แสดงสมรรถนะระดับ 1 และ • วางแผนเพื่อให้โอกาสผู้ใต้บังคับบัญชาแสดงความสามารถในการทำงาน • สามารถช่วยแก้ปัญหาที่เป็น	• วางแผนในการพัฒนาผู้ใต้บังคับบัญชาทั้งในระยะสั้นและระยะยาว • มอบหมายงานที่เหมาะสม รวมทั้งให้โอกาสผู้ใต้บังคับบัญชาที่จะได้รับการฝึกอบรมหรือพัฒนาอย่างสม่ำเสมอเพื่อสนับสนุนการเรียนรู้

ระดับของสมรรถนะ		พฤติกรรมบ่งชี้
	อุปสรรคต่อการพัฒนาศักยภาพของผู้ได้บังคับบัญชา	- มอบหมายหน้าที่ความรับผิดชอบในระดับตัดสินใจให้ผู้ได้บังคับบัญชาเป็นบางเรื่องเพื่อให้มีโอกาสริเริ่มสิ่งใหม่ ๆ หรือบริหารจัดการด้วยตนเอง - สามารถปรับเปลี่ยนทัศนคติเดิมที่เป็นปัจจัยขัดขวางการพัฒนาศักยภาพของผู้ได้บังคับบัญชา - สามารถเข้าใจถึงสาเหตุแห่งพฤติกรรมของแต่ละบุคคลเพื่อนำมาเป็นปัจจัยในการพัฒนาศักยภาพของผู้ได้บังคับบัญชาได้
ระดับ 3 สูงกว่าเป้าหมาย	- แสดงสมรรถนะระดับ 2 และ - ทำให้องค์การมหาชนมีระบบการสอนงานและการมอบหมายหน้าที่ความรับผิดชอบ	- สร้างและสนับสนุนให้มีการสอนงานและมีการมอบหมายหน้าที่ความรับผิดชอบอย่างเป็นระบบในองค์การมหาชน - สร้างและสนับสนุนให้มีวัฒนธรรมแห่งการเรียนรู้อย่างต่อเนื่องในองค์การมหาชน

3. รายละเอียดของการประเมินสมรรถนะทางการบริหารของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

จากข้อมูลข้างต้น จึงได้มีการกำหนดรายละเอียดของการประเมินสมรรถนะทางการบริหารของเลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ดังนี้

องค์ประกอบ การประเมิน	ประเด็นการประเมิน	เป้าหมาย	ผลการ ดำเนินงาน	ผลประเมิน (รายตัวชี้วัด)	สรุปผลประเมิน (รายองค์ประกอบ)
2.1 ผลงานของผู้อำนวยการองค์การมหาชน (Performance)					
2.1.1 สัญญาจ้าง เลขาธิการ คณะกรรมการ การรักษา ความมั่นคง ปลอดภัยไซเบอร์ แห่งชาติ	1) มีการจัดตั้งและบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้มีทรัพยากรบุคคล ระบบข้อมูลและองค์ความรู้เพื่อรองรับการปฏิบัติงาน รวมทั้งพัฒนาระบบการบริหารจัดการสารสนเทศและดิจิทัล และการสื่อสารประชาสัมพันธ์ให้เกิดการรับรู้แก่ผู้ที่เกี่ยวข้อง ภายในปี 2565	ได้รับผลคะแนนประเมินไม่น้อยกว่าร้อยละ 70			
	2) การจัดทำและดำเนินการตามนโยบาย แผน และยุทธศาสตร์เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์	ได้รับผลคะแนนประเมินไม่น้อยกว่าร้อยละ 70			
	3) การบริหารจัดการสำนักงานคณะกรรมการการรักษาความมั่นคง	ได้รับผลคะแนนประเมินไม่น้อย			

องค์ประกอบ การประเมิน	ประเด็นการประเมิน	เป้าหมาย	ผลการ ดำเนินงาน	ผลประเมิน (รายตัวชี้วัด)	สรุปผลประเมิน (รายองค์ประกอบ)
	ปลอดภัยไซเบอร์แห่งชาติให้เป็นไปตาม วัตถุประสงค์ของกฎหมาย นโยบาย มติ ของ กมช. กกม. และ กบส. และ กฎหมายที่เกี่ยวข้อง ภายในปี 2565	กว่าร้อยละ 70			
	4) แนวทางในการส่งเสริมและผลักดัน ให้หน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ หน่วยงานของรัฐ มี ความพร้อมในการป้องกัน รับมือ และ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์	ได้รับผลคะแนน ประเมินไม่น้อย กว่าร้อยละ 70			
	5) แนวทางและมาตรการในการพัฒนา สำนักงานคณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้มีความพร้อมในการรับมือกับภัย คุกคามทางไซเบอร์	ได้รับผลคะแนน ประเมินไม่น้อย กว่าร้อยละ 70			
	6) มีกฎหมายลำดับรองที่เกี่ยวข้องกับ การรักษาความมั่นคงปลอดภัยไซเบอร์ ที่สอดคล้องและเป็นไปตามมาตรฐานสากล	ได้รับผลคะแนน ประเมินไม่น้อย กว่าร้อยละ 70			
	7) มีรายงานสรุปผลการดำเนินงานของ การรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลกระทบอย่างมีนัยสำคัญต่อการ รักษาความมั่นคงปลอดภัยไซเบอร์ ของประเทศ	ได้รับผลคะแนน ประเมินไม่น้อย กว่าร้อยละ 70			
2.1.2 ผลการ ประเมินองค์กร	1) องค์ประกอบผลการประเมินผลการ ปฏิบัติงาน องค์ประกอบที่ 1 : ประสิทธิภาพ ผลการดำเนินงาน องค์ประกอบที่ 2 : ประสิทธิภาพ และความคุ้มค่าในการดำเนินงาน องค์ประกอบที่ 3 : ศักยภาพของ องค์การมหาชน องค์ประกอบที่ 4 : การควบคุมดูแล กิจการของคณะกรรมการองค์การ มหาชน	ประเมินโดย สำนักงาน ก.พ.ร.			
	2) การประเมินคุณธรรมและความ โปร่งใสในการดำเนินงานของ หน่วยงานภาครัฐ ประเมินโดย สำนักงาน ป.ป.ช.				

องค์ประกอบ การประเมิน	ประเด็นการประเมิน	เป้าหมาย	ผลการ ดำเนินงาน	ผลประเมิน (รายตัวชี้วัด)	สรุปผลประเมิน (รายองค์ประกอบ)
	3) ตัวชี้วัดผลกระทบ (impact) เพื่อติดตามผลสำเร็จเป็นรายปี (monitoring KPI) โดยให้องค์กรมหาชนรายงานผลตามตัวชี้วัดมายังสำนักงาน ก.พ.ร. แต่ไม่นำมาคำนวณคะแนน (นำผลการประเมินไปใช้ประกอบการรายงาน ครม.)				
2.1.3 งานอื่นๆ ที่คณะกรรมการ มอบหมาย	บริหารงานของสำนักงานให้เกิดผลสัมฤทธิ์ตามภารกิจของสำนักงานและตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบายของคณะรัฐมนตรีและ กมช. และข้อบังคับ นโยบาย มติ และประกาศของ กมช. กกม. และ กบส.	ได้รับผลคะแนนประเมินไม่น้อยกว่าร้อยละ 70			
2.2 สมรรถนะทางการบริหารของผู้อำนวยการองค์การมหาชน (Competency)					
สมรรถนะ ทางการบริหาร ของเลขาธิการ คณะกรรมการ การรักษา ความมั่นคง ปลอดภัยไซเบอร์ แห่งชาติ	1) ภาวะผู้นำ	ระดับ 3			
	2) วิสัยทัศน์	ระดับ 3			
	3) การวางกลยุทธ์	ระดับ 3			
	4) ศักยภาพเพื่อการปรับเปลี่ยน	ระดับ 3			
	5) การควบคุมตนเอง	ระดับ 3			
	6) การสอนงานและการมอบหมายงาน	ระดับ 3			

8. มิติผลกระทบ (Impact) ที่เกิดจากการดำเนินงานของตามวัตถุประสงค์ขององค์การมหาชน

8.1 สถานการณ์และแนวโน้มของภัยคุกคามทางไซเบอร์

จากปัญหาของภัยคุกคามไซเบอร์มีรูปแบบที่หลากหลาย ซับซ้อน และทวีความรุนแรงยิ่งขึ้น โดยเฉพาะภัยคุกคามไซเบอร์ที่มีแนวโน้มส่งผลกระทบต่อเศรษฐกิจ เช่น WannaCry ที่เป็นตัวอย่างของ Ransomware ซึ่งกระทบต่อระบบของทั่วโลกในหลายๆ ภาคส่วน จากความตระหนักในด้านความเสี่ยงบนโลกอินเทอร์เน็ตที่ทวีความรุนแรงมากขึ้นเรื่อยๆ อันเนื่องมาจากภัยคุกคามทางไซเบอร์ที่ซับซ้อนมีการขยายตัวเพิ่มมากขึ้น ย่อมส่งผลกระทบต่อหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือ “Critical Information Infrastructure (CII)” ของประเทศ ที่มีการใช้งานคอมพิวเตอร์หรือระบบคอมพิวเตอร์ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ซึ่งหากถูกโจมตีจากภัยคุกคามทางไซเบอร์แล้ว จะส่งผลกระทบและความสูญเสียอย่างร้ายแรงต่อประเทศอย่างมาก ทั้งในด้านเศรษฐกิจ สังคม การดำเนินชีวิตประจำวันของประชาชน ไปจนถึงความมั่นคงของชาติ รวมทั้ง ความไว้วางใจและความเชื่อมั่นย่อมได้รับผลกระทบอย่างมีนัยยะสำคัญ

และจากดัชนีความมั่นคงปลอดภัยไซเบอร์โลก (Global Cybersecurity Index : GCI) ของ ITU ในปี พ.ศ. 2561 นั้น ประเทศไทยอยู่ในอันดับที่ 35 (บางระดับอันดับซ้ำกัน) จาก 194 ประเทศ โดยที่เมื่อปี พ.ศ. 2560 ประเทศไทยอยู่ในอันดับที่ 22 จึงลงมาเกือบ 13 อันดับ (ลงประมาณเกือบ 60%) นอกจากนี้ เมื่อเปรียบเทียบกับประเทศสมาชิกในกลุ่มอาเซียนแล้ว ประเทศไทยอยู่อันดับที่ 3 รองจากสิงคโปร์ และมาเลเซีย ซึ่งมาตรการด้านหนึ่งที่ต้องเร่งผลักดันเนื่องจากยังอยู่ในระดับที่น่าเป็นห่วง คือ การมีหน่วยงานเพื่อดำเนินการกิจด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ของประเทศโดยตรง ดังนั้น เพื่อเป็นการยกระดับการจัดอันดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย การจัดตั้งสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติตามพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จึงเป็นเรื่องที่มีความจำเป็นและเร่งด่วน นอกจากนั้น แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติฉบับที่สิบสอง พ.ศ. 2560– 2564 ได้เล็งเห็นถึงความสำคัญของภัยคุกคามทางไซเบอร์ที่เพิ่มระดับความรุนแรงและมีความซับซ้อนในการโจมตีมากขึ้น ความเสียหายที่เกิดจากการอาชญากรรมและการโจมตีทางไซเบอร์จะมีผลอย่างร้ายแรง ซึ่งต้องให้ความสำคัญและมีมาตรการป้องกันภัยคุกคามทางไซเบอร์ให้สอดคล้องกับการเปลี่ยนแปลงทางสภาพแวดล้อม โดยเฉพาะการกำหนดกฎหมายและมาตรการที่เกี่ยวข้องกับความมั่นคงปลอดภัยบนโลกไซเบอร์ให้รัดกุมมากยิ่งขึ้นตั้งแต่ระดับชาติถึงระดับบุคคล

ประกอบกับประเทศไทยยังขาดบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์จำนวนมาก และต้องการเตรียมความพร้อมเพื่อรองรับภัยคุกคามจำนวนมากในอนาคต จึงเป็นนโยบายหลักของรัฐที่ต้องเร่งดำเนินการเพื่อป้องกันการโจมตีทางไซเบอร์ของประเทศไทย

ดังนั้น บทบาทของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงมีความสำคัญอย่างมากต่อเศรษฐกิจของประเทศและนโยบายรัฐบาล โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จะเป็นหน่วยงานกลางที่จะสร้างกลไกในการขับเคลื่อนการทำงานในการดูแลและรับมือภัยคุกคามไซเบอร์ รวมทั้งให้ความช่วยเหลือและสนับสนุนหน่วยงานภาครัฐ และหน่วยงานที่เป็นพื้นฐานสำคัญทางสารสนเทศเพื่อลดความเสี่ยงและบรรเทาความเสียหายจากภัยคุกคามที่จะเกิดขึ้น

8.2 บทบาทภารกิจของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อดำเนินงานตามนโยบายที่สำคัญเฉพาะด้านของรัฐบาลในการรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ โดยกำหนดมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดการกระทำหรือการดำเนินการใด ๆ โดยมีขอบเขตใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ นั้น

ซึ่งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีบทบาทสำคัญเพื่อเตรียมความพร้อมในการป้องกัน รับมือและจัดการปัญหาภัยคุกคามทางไซเบอร์ เสริมสร้างความเข้มแข็ง ในการดูแลความมั่นคงปลอดภัยไซเบอร์ของประเทศอย่างเป็นระบบ การสร้างความรู้ ความตระหนักให้แก่หน่วยงาน องค์กร และประชาชนทั่วไปให้สามารถดูแลตนเองได้ ตลอดจนการประสานความร่วมมือทั้งภายใน และระหว่างประเทศ ซึ่งสรุปบทบาทภารกิจของสำนักงานตามพระราชบัญญัติฯ ได้ดังนี้

1) งานด้านนโยบายและแผน

- เสนอแนะและสนับสนุนในการจัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
- เสนอแนะและสนับสนุนในการจัดทำนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- เสนอแนะและสนับสนุนในการจัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติ และในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์
- ติดตามและประเมินผลการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์
- สนับสนุนคณะกรรมการระดับชาติในการจัดทำนโยบายและแผนยุทธศาสตร์ระดับชาติ เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- ส่งเสริมให้เกิดแผนการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกัน อย่างเป็นระบบในองค์กรรวมทั้งการประสานงานภายในประเทศระหว่างหน่วยงานภาครัฐ ภาคเอกชน และการประสานงานกับต่างประเทศ

2) งานด้านมาตรฐานและการส่งเสริม

- จัดทำหลักเกณฑ์มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงแนวทางส่งเสริมการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชน
- จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้ง กำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทาง

ไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

- รวบรวม ผลิต แจกจ่ายงานข่าวกรองทางไซเบอร์ เพื่อสร้างความตระหนักรู้และลดช่องโหว่ จากการถูกโจมตีทางไซเบอร์ต่อสาธารณูปโภคพื้นฐานที่สำคัญของประเทศ

3) งานด้านการบริหารจัดการ

- ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือหน่วยงานที่เกี่ยวข้องในการปฏิบัติตาม นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความ มั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ หรือตามคำสั่งของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- เป็นศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thai National CERT) ในการติดตาม ฝ้าระวัง และประสานงานกับหน่วยงาน Sector-base CERT ต่าง ๆ อย่างเป็นระบบ
- ประสานงานและให้ความร่วมมือในการตั้งศูนย์กลางในการประสานความร่วมมือระหว่างหน่วยงาน เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานเอกชน ทั้งใน ประเทศและต่างประเทศ
- เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของประเทศ ซึ่งรวบรวมข้อมูลและนำมาวิเคราะห์อย่างเป็นระบบเพื่อเตรียมความพร้อมหรือ มาตรการรับมือต่อภัยคุกคามไซเบอร์ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน
- ทำความตกลงและร่วมมือกับองค์การหรือหน่วยงานทั้งในประเทศและ ต่างประเทศในกิจการ ที่เกี่ยวกับการดำเนินการตามหน้าที่และอำนาจของสำนักงาน เมื่อได้รับความเห็นชอบจาก คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้ รวมทั้งปัญหาและ อุปสรรคเสนอต่อคณะกรรมการเพื่อพิจารณา ทั้งนี้ ตามระยะเวลาที่คณะกรรมการกำหนด
- ประสานความร่วมมือกับหน่วยงานอื่นทั้งในประเทศและต่างประเทศที่เกี่ยวข้องกับการรักษา ความมั่นคงปลอดภัยไซเบอร์

4) งานด้านการรับมือภัยคุกคามไซเบอร์

- ประสานงานการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศตามมาตรา 52 และมาตรา 53
- ประสานงานและให้ความร่วมมือในการตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบ คอมพิวเตอร์ในประเทศและต่างประเทศในส่วนที่เกี่ยวข้องกับเหตุการณ์ที่เกี่ยวกับความมั่นคง ปลอดภัยไซเบอร์ และกำหนดมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์
- ดำเนินการและประสานงานกับหน่วยงานของรัฐและเอกชนในการตอบสนองและรับมือกับภัยคุกคาม ทางไซเบอร์ตามที่ได้รับมอบหมาย
- ฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับ ภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

- ดำเนินการและให้ความร่วมมือหรือช่วยเหลือในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยเฉพาะภัยคุกคามทางไซเบอร์ที่กระทบหรือเกิดแก่โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- ปฏิบัติการ ประสานงาน สนับสนุน และให้ความช่วยเหลือหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
- การจัดให้มีการซ้อมรับมือภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงานและภาคส่วนที่เกี่ยวข้องมีความพร้อม และความสามารถในการรับมือการจัดการปัญหา รวมถึงการติดต่อประสานข้อมูลตามแผนปฏิบัติการ เพื่อเกิดเหตุภัยคุกคามได้อย่างมีประสิทธิภาพ

5) งานด้านการวิจัยและการพัฒนา

- ศึกษา และวิจัยข้อมูลที่สำคัญสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ
- ศึกษา และวิจัยเพื่อการพัฒนาเทคโนโลยีในการสนับสนุนการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งเป็นการวิจัยและพัฒนากระบวนการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ บริการตรวจสอบ หรือวิเคราะห์ภัยคุกคาม มัลแวร์ และช่องโหว่ของระบบหรืออุปกรณ์ที่ใช้ในการให้บริการ เพื่อป้องกันภัยคุกคามไซเบอร์
- การศึกษา วิจัย และพัฒนางานด้านการตรวจพิสูจน์พยานหลักฐานดิจิทัล (Digital Forensic) ให้มีความถูกต้องและน่าเชื่อถือตามมาตรฐานที่ได้รับการยอมรับรวมถึงการพัฒนานวัตกรรมในด้านดังกล่าว

6) งานด้านกฎหมายและการบังคับใช้

- เพื่อดูแลประเด็นทางกฎหมายที่เกี่ยวข้องในขั้นตอนต่างๆ สำหรับการดำเนินมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการปรับปรุงหรือจัดทำกฎหมาย หลักเกณฑ์ มาตรฐาน หรือแนวปฏิบัติ (self-regulation) ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่รองรับรูปแบบและลักษณะของภัยคุกคามที่เปลี่ยนแปลงไป ตามวิวัฒนาการของเทคโนโลยี ซึ่งสอดคล้องกับหลักสากล

7) งานด้านพัฒนานวัตกรรม

- เสริมสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้าง ความตระหนักรู้ด้านสถานการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ร่วมกัน เพื่อให้มีการดำเนินการเชิงปฏิบัติการที่มีลักษณะบูรณาการและเป็นปัจจุบัน
- ส่งเสริม สนับสนุน และดำเนินการในการเผยแพร่ความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ตลอดจนดำเนินการฝึกอบรมเพื่อยกระดับทักษะ ความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- การพัฒนาทักษะในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศและตอบสนองต่อภัยคุกคามได้อย่างทัน่วงที
- การอบรม และการเผยแพร่ความรู้ รวมถึง การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้เกิดขึ้นทั้งในระดับหน่วยงาน องค์กร และประชาชนทั่วไป

8.3 แผนปฏิบัติการ ระยะ 3 ปี (พ.ศ. 2563 – 2565) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้จัดทำแผนปฏิบัติการ ระยะ 3 ปี (พ.ศ. 2563 – 2565) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยมีวัตถุประสงค์เพื่อใช้เป็นกรอบแนวทางการดำเนินงานของหน่วยงานภายในสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติในการพัฒนาองค์กรเพื่อขับเคลื่อนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนด และให้สอดคล้องกับยุทธศาสตร์ชาติ ระยะ 20 ปี แผนแม่บทภายใต้ยุทธศาสตร์ชาติ แผนการปฏิรูปประเทศ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2562 -2565) นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ. 2561 - 2580) แผนปฏิบัติการด้านดิจิทัลเพื่อเศรษฐกิจและสังคมระยะ 5 ปี (พ.ศ. 2562 - 2565) ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560 - 2564) และแผนเตรียมพร้อมแห่งชาติ (พ.ศ. 2560 - 2564)

โดยแผนปฏิบัติการระยะ 3 ปี (พ.ศ. 2563 – 2565) ของสำนักงานฉบับนี้ เป็นการกำหนดแผนงาน โครงการสำคัญที่ครอบคลุมระยะเวลาการดำเนินงานใน 3 ปี คือ พ.ศ. 2563 – 2565 เพื่อช่วยให้เห็นภาพรวมของแนวทางการพัฒนาสู่การดำเนินการของหน่วยงานอย่างเป็นระบบ เพื่อการพัฒนาประเทศให้มีความมั่นคงและมีขีดความสามารถในการรับมือต่อภัยคุกคามทางไซเบอร์ในทุกมิติ

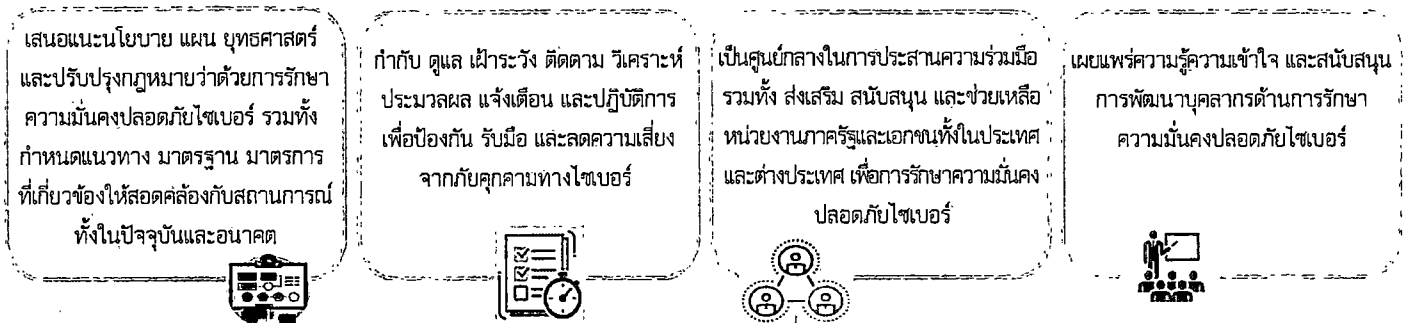
วิสัยทัศน์

"เป็นผู้นำในการขับเคลื่อนในการบริหาร
จัดการความมั่นคงปลอดภัยไซเบอร์ของประเทศ
ที่มีประสิทธิภาพพร้อมตอบสนองต่อ
ภัยคุกคามไซเบอร์ทุกมิติ"

แผนปฏิบัติการ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พ.ศ.2563 - 2565

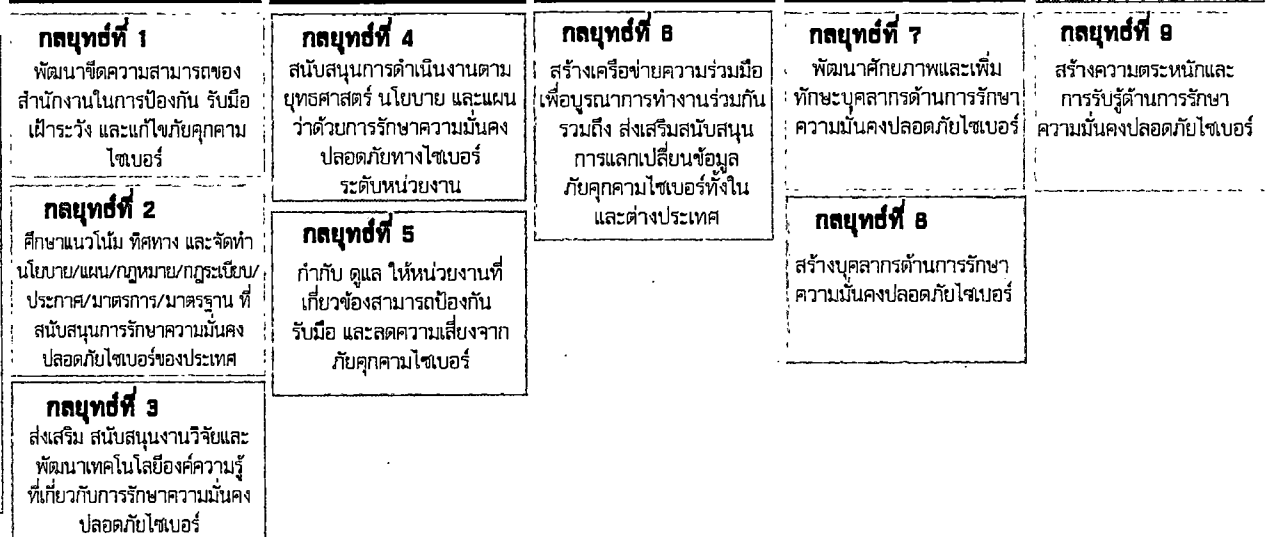
พันธกิจ



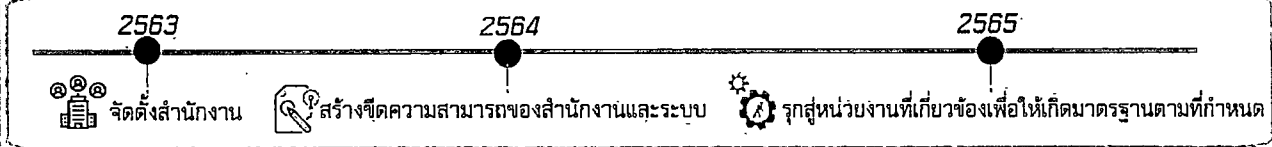
เป้าหมาย



กลยุทธ์องค์กร



แนวทางขับเคลื่อนระยะ 3 ปี



ผลกระทบ :

ประเทศไทยมีความมั่นคงและมีขีดความสามารถในการรับมือต่อภัยคุกคามทางไซเบอร์ในทุกมิติ

โดยการดำเนินงานป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ของประเทศไทยนั้น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จะเป็นหน่วยงานสำคัญทางด้านความมั่นคงปลอดภัยไซเบอร์ซึ่งเป็นหน่วยงานกลางในการกลยุทธ์/ยุทธวิธีในการแก้ไขปัญหาด้านความมั่นคงทางไซเบอร์ให้ครอบคลุมสภาพปัญหาของภัยคุกคามทางไซเบอร์ ที่มีการการโจมตีต่อกลุ่มหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานภาครัฐ กระทั่งประชาชนรวมทั้งอาจส่งผลกระทบต่อความมั่นคง โดยการดำเนินงานต้องสอดคล้องกับยุทธศาสตร์ชาติ ระยะ 20 ปี แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นความมั่นคง กล่าวคือ แนวคิดในการดำเนินการแก้ไขปัญหาที่สำคัญ ประกอบด้วย (1) กำหนดแนวความคิด มาตรการ มาตรฐาน ระบบบริหารจัดการในการป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ในภาพรวม (2) จัดองค์กร โครงสร้าง อำนาจหน้าที่ ชัดความสามารถในการป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ (3) กำหนดระบบบริหารจัดการในแต่ละระดับให้ชัดเจน (4) เสริมสร้างและพัฒนาระบบการรายงานในสถานการณ์ฉุกเฉิน (5) ยกระดับแนวความคิดในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (6) พัฒนาการป้องกันแก้ไขปัญหาการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคง (7) สร้างความตระหนักรู้ให้แก่ประชาชนและหน่วยงาน (8) ปรับปรุงแก้ไขกฎหมายที่เกี่ยวข้อง และ (9) พัฒนาศักยภาพบุคลากรและเทคโนโลยีให้ทันสมัยพร้อมรองรับสถานการณ์ทุกรูปแบบ โดยมีเป้าหมายเพื่อให้สามารถแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์ที่อาจส่งผลกระทบต่อการบริหารและพัฒนาประเทศ ให้สำเร็จลุล่วงด้วยความรวดเร็วทันต่อสถานการณ์

ตัวอย่างการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในการขับเคลื่อนการทำงานในการดูแลและรับมือภัยคุกคามไซเบอร์ รวมทั้งให้ความช่วยเหลือและสนับสนุนหน่วยงานภาครัฐ และหน่วยงานที่เป็นพื้นฐานสำคัญทางสารสนเทศเพื่อลดความเสี่ยงและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยมีรายละเอียดตามภาคผนวก

ภาคผนวก

Maze Ransomware โจมตี
รัฐวิสาหกิจกลุ่มพลังงานขนาดใหญ่
(มิถุนายน 2563)

การไฟฟ้า ยอมรับ โดนมัลแวร์เรียกค่าไถ่โจมตี ทำแอปล่มข้ามอาทิตย์!

เด่นออนไลน์



18 มิ.ย. 2563 - 17:33 น.



👍 2.5 พัน

ความคิดเห็น 144 รายการ แชร์ 256 ครั้ง



ประกาศด่วน

ขณะนี้กองโกลาไลระบบไฟฟ้า และขอใช้ไฟฟ้าได้ ทุกแห่งตาม
เนื่องจาก ระบบขัดข้อง จึงขอให้ พก. ตัวของระบบ Server
หยุดการเชื่อมระบบเครื่องใช้ไฟฟ้าทั้งหมด เพื่อทำการซ่อมแซม (โดยไม่มีการแจ้งเตือน)

เมื่อระบบสามารถใช้งานได้ตามปกติ
การไฟฟ้าส่วนภูมิภาคจะดำเนินการแจ้งเตือน
จะแจ้งให้ทราบโดยเร็วที่สุด
(ขออภัยในความไม่สะดวก)

สอบถามรายละเอียดเพิ่มเติมได้ที่ 02 581 5373, 02 581 1532 (ในวัน และเวลาราชการเท่านั้น)
หมายเลขโทรสาร 1129 ตลอด 24 ชั่วโมง

By CYBLEINC JUNE 19, 2020 @ 8:54 PM

MAZE RANSOMWARE OPERATORS ALLEGEDLY STRUCK PROVINCIAL ELECTRICITY AUTHORITY AND MARK'S PLUMBING PARTS – DATA LEAK!!

Update as of 06/19/2020: Maze ransomware operators, who are one of the well-known ransomware groups targeted two well-established organisations and leaked their confidential data on their website.

Published on June 19, 2020 at 14387 Views



Attackers hit Thai power authority
using Maze ransomware



การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

ที่ มท 5312.5/42913

ฝ่ายสารสนเทศ
การไฟฟ้าส่วนภูมิภาค
200 ถนนงามวงศ์วาน แขวงลาดยาว
เขตจตุจักร กรุงเทพฯ 10900

10 กรกฎาคม 2563

เรื่อง รายงานภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ และขอรับการสนับสนุนเจ้าหน้าที่ผู้เชี่ยวชาญ
เรียน ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม/ผู้บริหารสำนักงานคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ

ด้วยเมื่อวันที่ 13 มิถุนายน 2563 ระบบสารสนเทศของการไฟฟ้าส่วนภูมิภาค ถูกโจมตีด้วย Maze Ransomware เป็นเหตุให้เครื่องคอมพิวเตอร์แม่ข่ายในศูนย์ข้อมูลของการไฟฟ้าส่วนภูมิภาค (PEA Data Center) และเครื่องคอมพิวเตอร์ลูกข่ายทั้งในสำนักงานใหญ่และสำนักงานเขตจำนวนมากได้รับความเสียหาย ถูก Hacker เข้าควบคุม ไฟล์บางส่วนถูกเข้ารหัส (Encrypt) พร้อมกับการขึ้นข้อความเรียกค่าไถ่แลกกับการถอดรหัส (Decrypt) เพื่อให้สามารถเปิดใช้งานไฟล์ได้ตามปกติ การไฟฟ้าส่วนภูมิภาคจึงขอรายงาน สถานการณ์ภัยคุกคามทางไซเบอร์ และความเสียหายที่เกิดขึ้นโดยสรุป ดังนี้

1. โดเมน pea.co.th ไม่สามารถใช้งานได้ เครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่ควบคุม โดเมนได้รับความเสียหายทั้งหมด (เครื่องคอมพิวเตอร์แม่ข่าย Active Directory Server และ DNS Server)
2. เครื่องคอมพิวเตอร์ควบคุมบริหารจัดการ Virtual Server (VCenter) ได้รับความเสียหายไม่สามารถเข้าถึงได้ ทำให้ไม่สามารถตรวจสอบ Virtual Server ของการไฟฟ้าส่วนภูมิภาค ทั้งหมดได้ (รวมถึงเครื่องคอมพิวเตอร์ข่ายระบบสำรอง/กู้คืนข้อมูล)
3. พบเครื่องคอมพิวเตอร์ลูกข่ายที่เปิดใช้งานในวันที่ 13 มิถุนายน 2563 เช่น เครื่องรับชำระเงินที่หน้างาน (BPM Client) และเครื่องคอมพิวเตอร์ลูกข่ายภายในสำนักงานใหญ่ และสำนักงานเขต

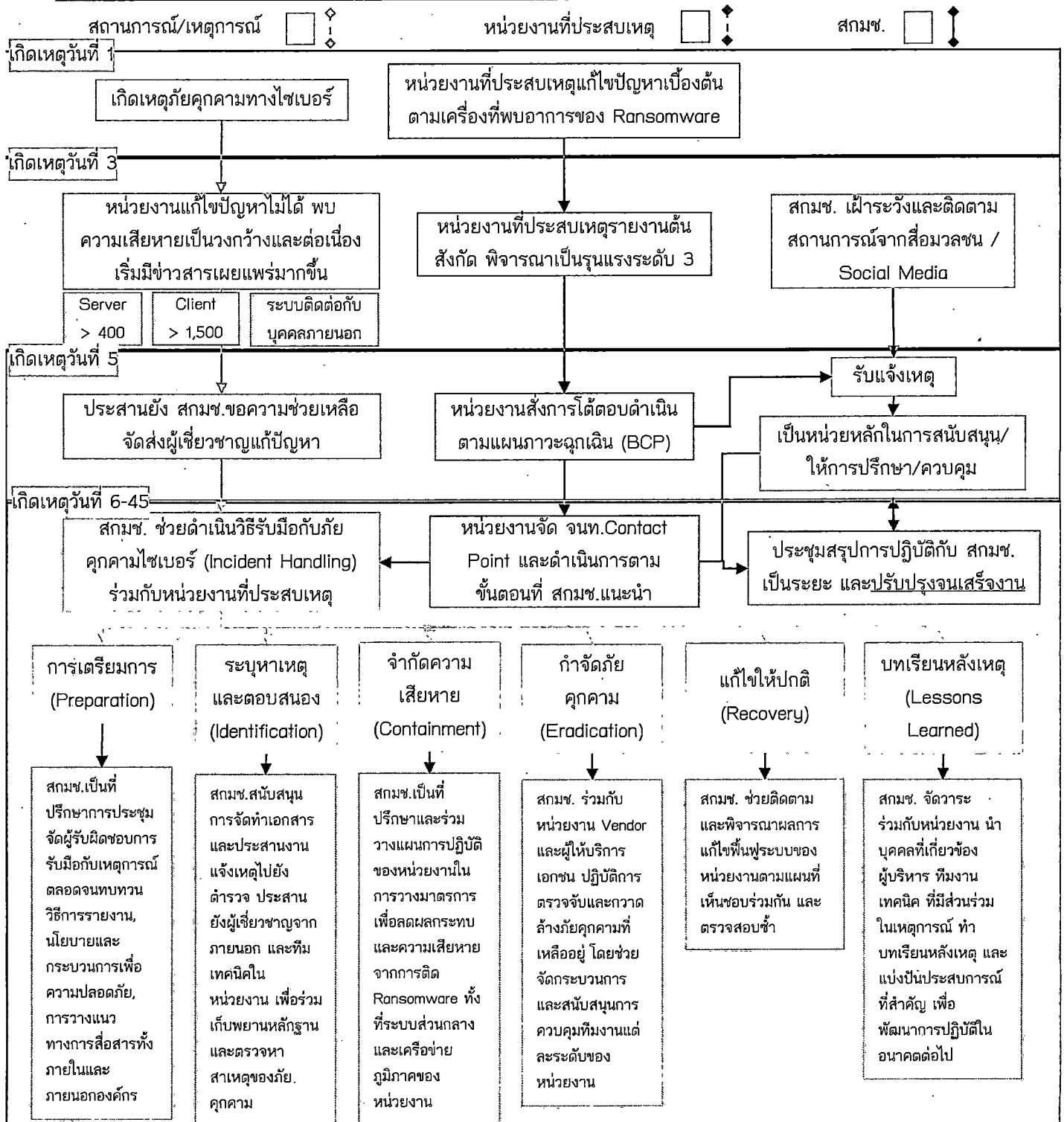
เพื่อให้การแก้ไขปัญหาของการไฟฟ้าส่วนภูมิภาค เป็นไปโดยมีประสิทธิภาพและเป็นการเร่งด่วนหันต่อ สถานการณ์ จึงใคร่ขอเสนอแนะให้จากท่านสว.ผู้เชี่ยวชาญในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยพิจารณาอนุญาตให้ หันตำรวจโท ณัทกฤษ พรหมจันทร์ ซึ่งเคยให้คำแนะนำที่เป็นประโยชน์ต่อการลด ความเสี่ยง และแก้ไขปัญหาในทางปฏิบัติตลอดช่วงที่ผ่านมา มาร่วมเป็นคณะทำงานในการจัดการแก้ไขปัญหา จนกว่าระบบจะสามารถใช้งานได้ตามปกติโดยเร็วต่อไป จักเป็นการขอบพระคุณยิ่ง

ขอแสดงความนับถือ

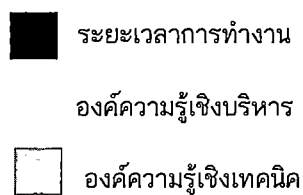
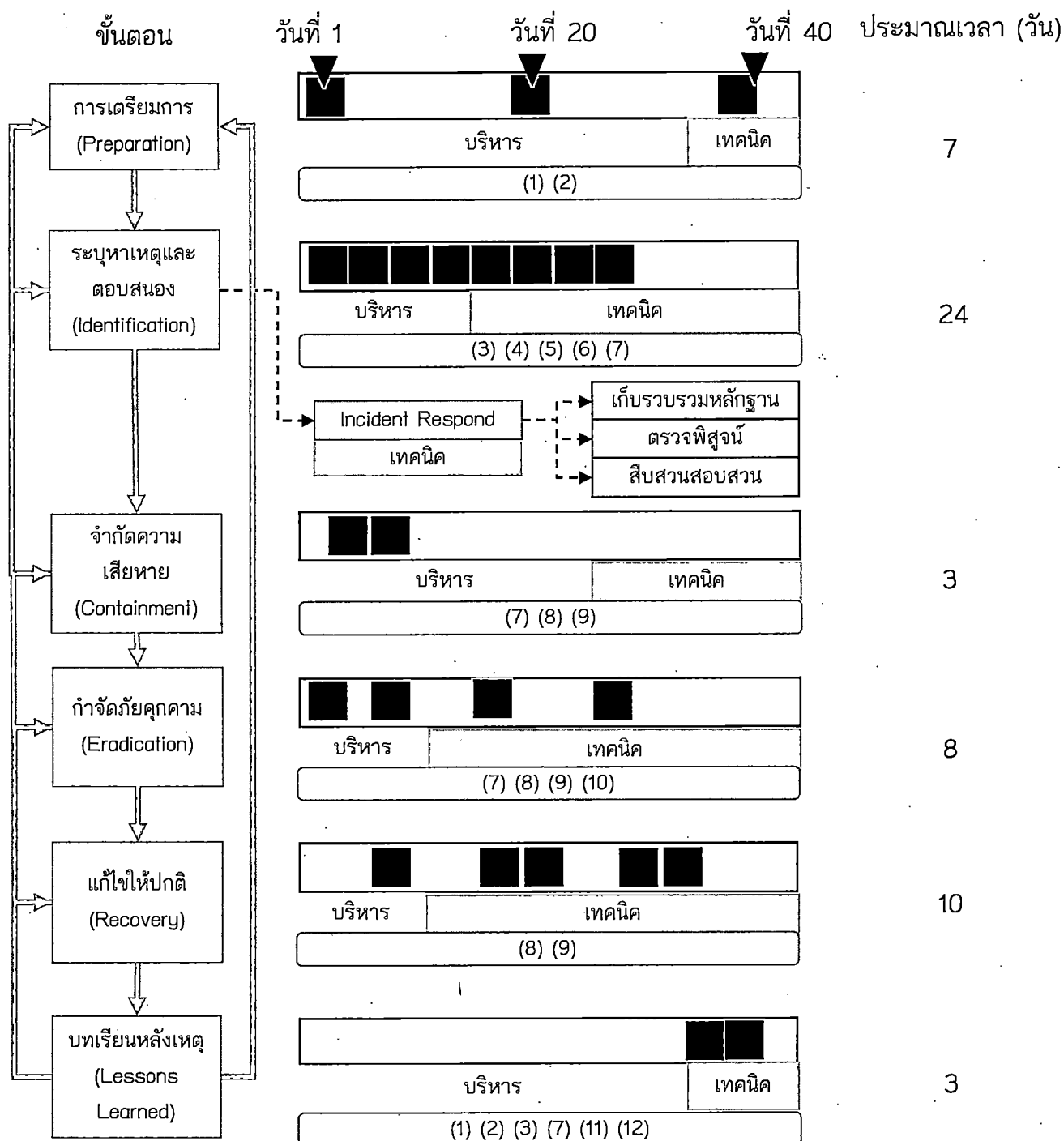
(นางฐิติรัตน์ พละสร)
ผู้อำนวยการฝ่ายสารสนเทศ

เมื่อ ม.ย.2563 เกิดเหตุภัยคุกคามทางไซเบอร์ Maze Ransomware โจมตีระบบของรัฐบาลวิสาหกิจกลุ่มพลังงานขนาดใหญ่ มีการขู่เรียกค่าไถ่แลกกับการไม่เปิดเผยข้อมูลที่ถูกขโมยไปแล้วของหน่วยงานจำนวนมาก ในขณะเดียวกัน ผลกระทบจาก Ransomware ดังกล่าว ยังทำให้เครื่องแม่ข่าย และลูกข่ายจำนวนรวมประมาณ 2,000 เครื่อง ใช้งานไม่ได้ ส่งผลต่อเนื่องไปยังระบบบริหารการเงินออนไลน์ทั่วประเทศไม่สามารถทำงานได้ตามปกติ

หลังเกิดเหตุ 5 วัน สกมช.ได้รับการประสานให้สนับสนุนการแก้ปัญหา ทีมงาน สกมช.ลงพื้นที่ดำเนินวิธีรับมือกับภัยคุกคามไซเบอร์ (Incident Handling) ร่วมกับหน่วยงานที่ประสบเหตุ ตั้งแต่ขั้นตอนเตรียมการไปจนถึงการจัดทำบทเรียนหลังเหตุเป็นระยะเวลาต่อไปอีกประมาณ 40 วัน จึงสามารถระบุถึงสาเหตุ พฤติกรรมคนร้าย และกู้คืนระบบหลักให้ใช้งานได้ตามปกติ ความเสียหายภาพรวมเกิดจากระบบคอมพิวเตอร์ที่เกี่ยวข้องกับธุรกิจหลัก (Core Business) ทำงานไม่ได้ประมาณ 1 สัปดาห์ และต้องใช้เวลาในการแก้ไขเครื่องคอมพิวเตอร์จำนวนมากประมาณ 1 เดือน และข้อมูลขององค์กรและผู้เกี่ยวข้องรั่วไหลสู่โลกอินเทอร์เน็ตจำนวน 20GB มีผู้เกี่ยวข้องมากกว่า 300,000 คน หน่วยงานยังไม่มีประเมินความเสียหายเป็นตัวเงิน



บทบาทของ สกมช. การสนับสนุนการดำเนินวิธีรับมือกับภัยคุกคามไซเบอร์
(Incident Handling) ร่วมกับหน่วยงานที่ประสบเหตุ
กรณี Maze Ransomware โจมตีรัฐวิสาหกิจกลุ่มพลังงานขนาดใหญ่



ทักษะ/เทคนิคทางอาชีพที่ใช้ในแต่ละขั้นตอน

- | | |
|--|---|
| (1) Information Systems Security Manager | (7) Blue Team Technician |
| (2) Information Technology (IT) Director | (8) Systems Administrator |
| (3) Incident Analyst | (9) Network Administrator |
| (4) Computer Forensic Analyst | (10) Intrusion Detection System Administrator |
| (5) Computer Crime Investigator | (11) Information Manager |
| (6) Incident Responder | (12) Information Security Manager |

Spade Ransomware โจมตีระบบ
คอมพิวเตอร์โรงพยาบาลของรัฐ
(กันยายน 2563)

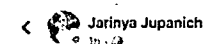
M ข่าวในพระราชสำนัก [ภาวะติด COVID-19](#) [การเมือง](#) [เศรษฐกิจ](#) [หุ้น-การเงิน](#) [บริหารการเงิน](#) [ในประเทศ](#) [ภูมิภาค](#) [ต่างประเทศ](#) [การศึกษา](#)

ไลน์สไตร์ ~ กิ๊วก ~ มัสมิง ~ INTERNATIONAL นิสัรปัทธการณั้ คณิย ประยัณ โพล – สัการคณณัณ แฉกคณังสั ~ อีนา ~

Unofficial Indian

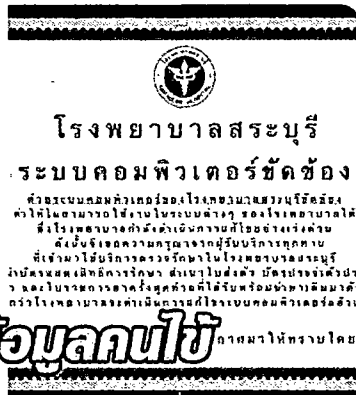
รพ.สระบุรีโดนแฮกข้อมูลรักษาคนไข้-เรียกค่าไถ่
หน่วยงานช่วยตัวย

วันที่ 9 กันยายน 2563 - 09:25 น.



©ตอนนี่คอมพิวเตอร์โดนด้วยransomware เรียก
ค่าไถ่ด้วยเงินจำนวนหนึ่ง แลกรับข้อมูล ตอนนี่คอมพิวเตอร์ ใ
งานอะไรไปไม่ได้เลย ขู่ข้อมูลต่างๆของคนใช้ไม่ให้
@วันนี้ไปเจอ opdsเข้า แลแต่ถ้าได้ไม่เน้อ เมือจะจาดัด
ทุกอย่าง ตั้งแต่ห้องบัตร ห้องจะเกิดก็เจาะแล้ว คือ
report labมาปะในOpd เจ้าหน้าที่ต้องวิ่งไปเอาอบเป็น
ระยะ

@โอเช่แหวว ที่ปกติก็แน่นอนอยู่แล้ว ยิงหนัก แต่ที่หนักใจคือ
ประวัติอะไรที่มี ก็พิมพ์ไว้ในคอมเมนต์ละมิดมิดมาก ดันชี้ว่า
ได้ความรู้ว่า ต้องถามแบบไขว่ถามแบบโหละโละ ไข้อย่างไร??
ถ้าตอบได้จะง่ายกว่าตอบไม่ได้ แต่ฉันดันไปถูก80%
ไม่ได้ฉายาดีขึ้นมา ต้องเอาเมียมาถามคนเดียว ว่างถึงมี
การถาม ใช้เวลาถามเขาเรื่อยๆตลอด จากหนึ่งข้อไป
ระบบถามจนเขียนยาวๆ
ความเขาลึกซึ้งๆ ที่มัน **โดนเทออก**
ถกกันยี่สิบ ผู้มีปัญญารู้ (เพี้ยนๆ) เหนือใจว่า ทำคนเดียวทุก
คน ทบทวนแล้วปรากฏหะหะ โทษแล้วละที่เล่น



បដិច្ចសារក្រុម

นพิตินาฎิโก ข้าราชการตํารวจสูงที่สุดมีตำแหน่ง คือประมุขบรรณ
เทศไนโรเบียชานา เช่นทางเทศรัฐ ตํารวจเทศนิเทศชน คุมบัตตมุตตนิเทศ
มตนิเทศเทศนิเทศ Khaosod English Malichon Investor Relation
รณนงนทณนา.

กิจกรรม

มัติชนออนไลน์

បាវចនាបទដ្ឋាន



"ชาย ฉากาพร" ถูกรางวัลเลขท้าย 15 ใบ



ไฉนที่ทีมช้างบน 'สเปร์ส' มุกสวย
'เซฟ'เยวี่ 3-1 ขยับรั้งที่ 4 ทรูเมียร์
ลีก



เจสันศรี ขอโทษหึงน้ำดา ปม
คราาเพลงคล้าย Safeplanet
เผย แอ่ยากเป็น 'โมกัไลฮัน'

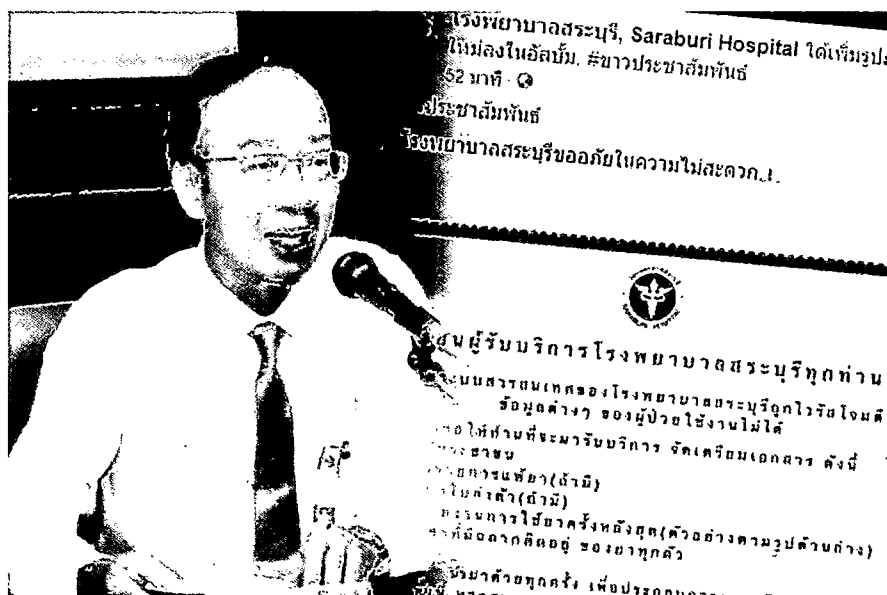


แม่เต๋ารักลูกสาว 17 คัมภีร์ปรศนาใน
หอวิเศษ พนมทอนล่างเป็ลือยเป็ล้า
กิดนพาศิลา

ผอ.รพ.สระบุรีรับถูกแยกจริง ปิดเจริตค่าไถ่6.3หมื่นล้าน

“ผอ.รพ.สระบุรี” ยอมรับคอมพิวเตอร์โรงพยาบาลถูกไวรัสเรียกค่าไถ่จริง แต่ยังปิดถูกเรียกเงิน 2 แสนบิตคอยน์ หรือราว 6.3 หมื่นล้านบาท ขอปชช.มารับบริการ พบกัณฑ์-โบส่งตัว เอกสารการแพทย์ พร้อม ใบรายการยารอบสตัยติดตัว

พธที่ 9 กันยายน 2563 เวลา 11.00 น.



เมื่อวันที่ 9 ก.ย. นพ.อนันต์ กมลเนตร ผอ.รพ.สระบุรี กล่าวถึงกรณีที่มีการเผยแพร่ในโซเชียลมีเดียต่างๆที่ รพ.สระบุรี โดน Ransomware แลกข้อมูลและเรียกค่าไถ่ 2 แสนมิตคอยน์ หรือราว 6.3 หมื่นล้านบาท ว่า ข้อมูลเบื้องต้นก่อน ระบบคอมพิวเตอร์รพ.สระบุรีขัดข้องจากการโดน Ransomware จริง แต่ในเรื่องของการเรียกค่าไถ่โดยต้องจ่าย 2 แสนมิตคอยน์ เพื่อให้ได้ข้อมูลคืนนั้นไม่จริง ขณะนี้ยังไม่ใครติดต่อมาในลักษณะดังกล่าวแต่อย่างใด



ที่ สป ๐๐๓๒.๑/๑๒๘๓๕

โรงพยาบาลสระบุรี
อำเภอเมือง จังหวัดสระบุรี ๑๘๐๐๐

๑๔ กันยายน ๒๕๖๓

เรื่อง รายงานเหตุภัยคุกคามทางไซเบอร์ และขอรับการสนับสนุนเจ้าหน้าที่ผู้เชี่ยวชาญ

เรียน ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และเลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ด้วยเมื่อวันที่ ๕ กันยายน ๒๕๖๓ เวลาประมาณ ๐๕.๓๑ น. ระบบสารสนเทศของโรงพยาบาลสระบุรี ได้ถูก Ransomware โจมตี เบื้องต้นพบว่า มีไฟล์ข้อมูลเกี่ยวกับการรักษาพยาบาล เช่น ประวัติการรักษาพยาบาล รายการยาที่ผู้ป่วยได้รับ เป็นต้นบางส่วนถูกเข้ารหัส (Encrypt) พร้อมกับขึ้นข้อความเรียกร้องค่าไถ่แลกกับการถอดรหัส (Decrypt) และมีการแพร่กระจายไปยังข้อมูลส่วนที่มีการสำรองไว้ เป็นเหตุให้ระบบและข้อมูลคอมพิวเตอร์ของโรงพยาบาลไม่สามารถใช้งานได้ตามปกติ โรงพยาบาลสระบุรี จึงรายงานเหตุดังกล่าวให้ทราบ และความเสียหายจากภัยคุกคามทางไซเบอร์ให้ท่านทราบ โดยสรุปเป็นดังนี้ คือ

๑. ฐานข้อมูลผู้ป่วย ไม่สามารถใช้งานได้
๒. ภาพสแกนเวชระเบียนผู้ป่วยเสียหายทั้งหมด
๓. เครื่องแม่ข่าย ให้บริการไม่ได้
๔. ระบบเครือข่าย/ระบบโทรศัพท์ ไม่สามารถใช้งานได้

ภายหลังเกิดเหตุ เมื่อวันที่ ๙ กันยายน ๒๕๖๓ โรงพยาบาลสระบุรีได้ติดต่อไปยังศูนย์ไซเบอร์กองทัพอากาศ ได้กรุณาจัดส่งทีมงานผู้เชี่ยวชาญจากศูนย์ไซเบอร์กองทัพอากาศ มาให้การช่วยเหลือในขั้นต้น ซึ่งต่อมาทางอากาศเอก อมร ชมเชย ผู้อำนวยการกองปฏิบัติการ ศูนย์ไซเบอร์กองทัพอากาศ หัวหน้าชุดทำงาน ได้แนะนำเจ้าหน้าที่ที่มีประสบการณ์ในการรับมือภัยคุกคามทางไซเบอร์ที่อยู่ในสังกัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้แก่ พันตำรวจโท ณัฏฐกฤษ พรหมจันทร์ และทีมผู้เชี่ยวชาญจาก EDTA นำโดยคุณพรพรม ประภาภิตติกุล มาประกอบกำลังเป็นทีมปฏิบัติการหลักร่วมกับโรงพยาบาลสระบุรีจนถึงปัจจุบัน

ทั้งนี้ เพื่อให้การแก้ไขปัญหาของโรงพยาบาลสระบุรี เป็นไปโดยมีประสิทธิภาพ ลุล่วง ทันท่วงที สถานการณ์ จึงใคร่ขออนุเคราะห์ท่านพิจารณาอนุญาตให้ พันตำรวจโท ณัฏฐกฤษ พรหมจันทร์ ร่วมเป็นคณะทำงานในการแก้ไขปัญหาที่เกิดขึ้นดังกล่าวต่อเนื่องไป จนกว่าระบบจะสามารถใช้งานได้ตามปกติต่อไป และถือโอกาสขอขอบพระคุณท่านที่กรุณาให้การสนับสนุนทางโรงพยาบาลในห้วงที่ผ่านมา มา ณ โอกาสนี้ด้วย

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นายอนันต์ กมลเนตร)

ผู้อำนวยการโรงพยาบาลสระบุรี

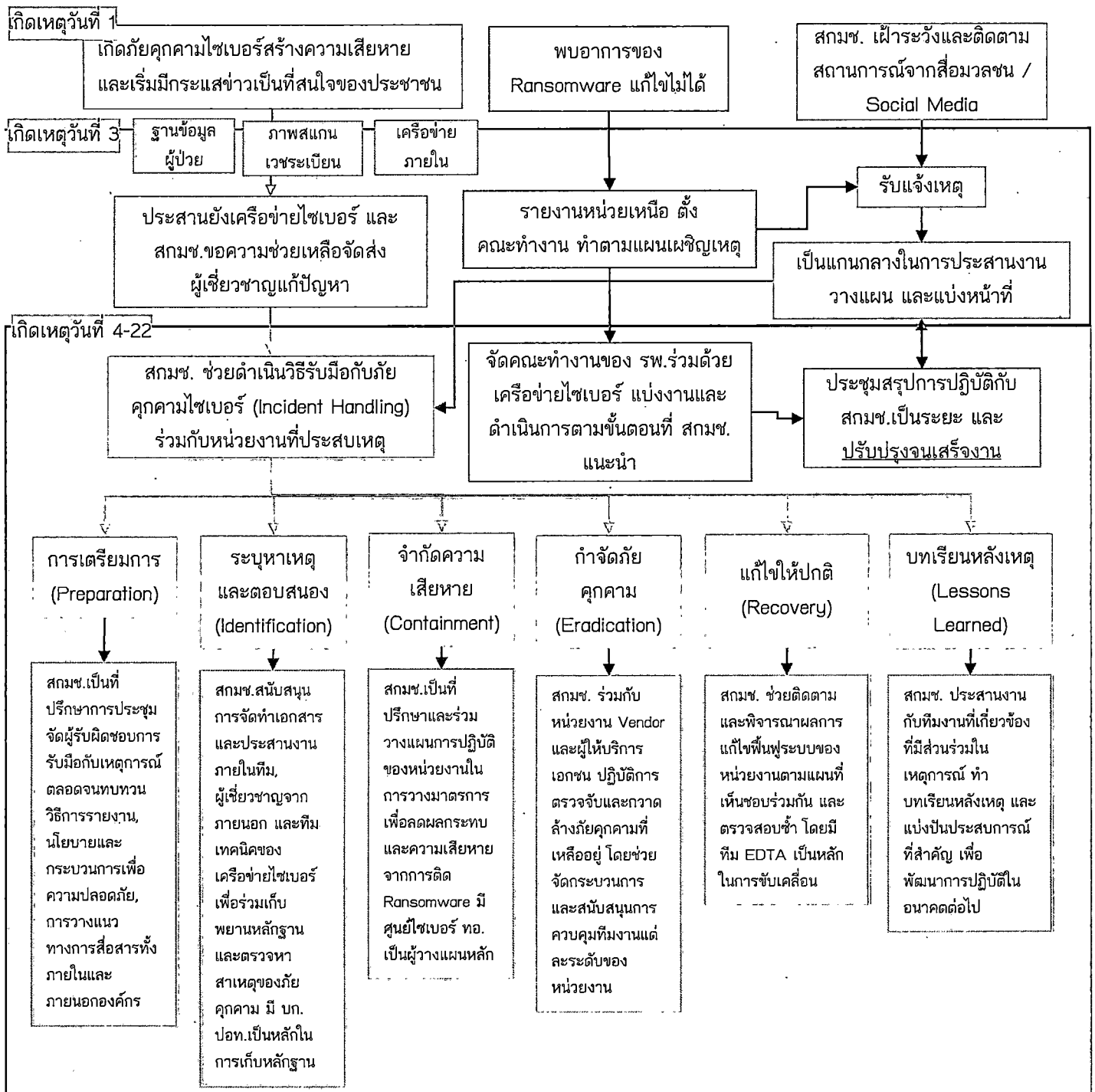
เมื่อ ก.ย.2563 เกิดเหตุภัยคุกคามทางไซเบอร์ Spade Ransomware โจมตีระบบคอมพิวเตอร์โรงพยาบาลของรัฐ ตามข้อมูลข่าวสารที่ปรากฏตามสื่อมวลชนว่า มีคนร้ายใช้ Ransomware โจมตีระบบของโรงพยาบาล เรียกค่าไถ่จำนวนหนึ่งแลกกับการปลดล็อกข้อมูล ต่อมา โรงพยาบาลได้โพสต์แจ้งว่าคอมพิวเตอร์ของโรงพยาบาลเกิดขัดข้องทำให้ไม่สามารถใช้ระบบต่างๆได้ จนกลายเป็นกระแสโด่งดังและเป็นที่สนใจของประชาชนทั่วไป หลังเกิดเหตุ 2 วัน สกมช.ได้รับการติดต่อให้เข้าดำเนินการช่วยเหลือเพื่อแก้ไขสถานการณ์ดังกล่าว

สกมช.ลงพื้นที่ดำเนินการวิธีการรับมือกับภัยคุกคามไซเบอร์ (Incident Handling) ตั้งแต่การปรับปรุงการสื่อสารในการแถลงข่าวอย่างเป็นทางการ และมีบทบาทหลักเป็นแกนกลางในการวางแผนประสานงานกับหน่วยงานที่เกี่ยวข้อง ได้แก่ ศูนย์ไซเบอร์ กองทัพอากาศ จนท. EDTA สก.เมืองสระบุรี และ บก.ปอท. โดยนำทีมแบ่งหน้าที่ตามขีดความสามารถของกำลังพลที่ร่วมสนับสนุน จนสามารถระบุสาเหตุของภัยคุกคาม ตรวจล้างสิ่งแปลกปลอมออกจากระบบเดิม และสนับสนุนการสร้างระบบเครือข่ายขนานให้กลับมาใช้งานได้ ใช้เวลาประมาณ 20 วัน ทั้งนี้ หน่วยงานไม่มีการประเมินความเสียหายเป็นต้นทุนแต่อย่างใด

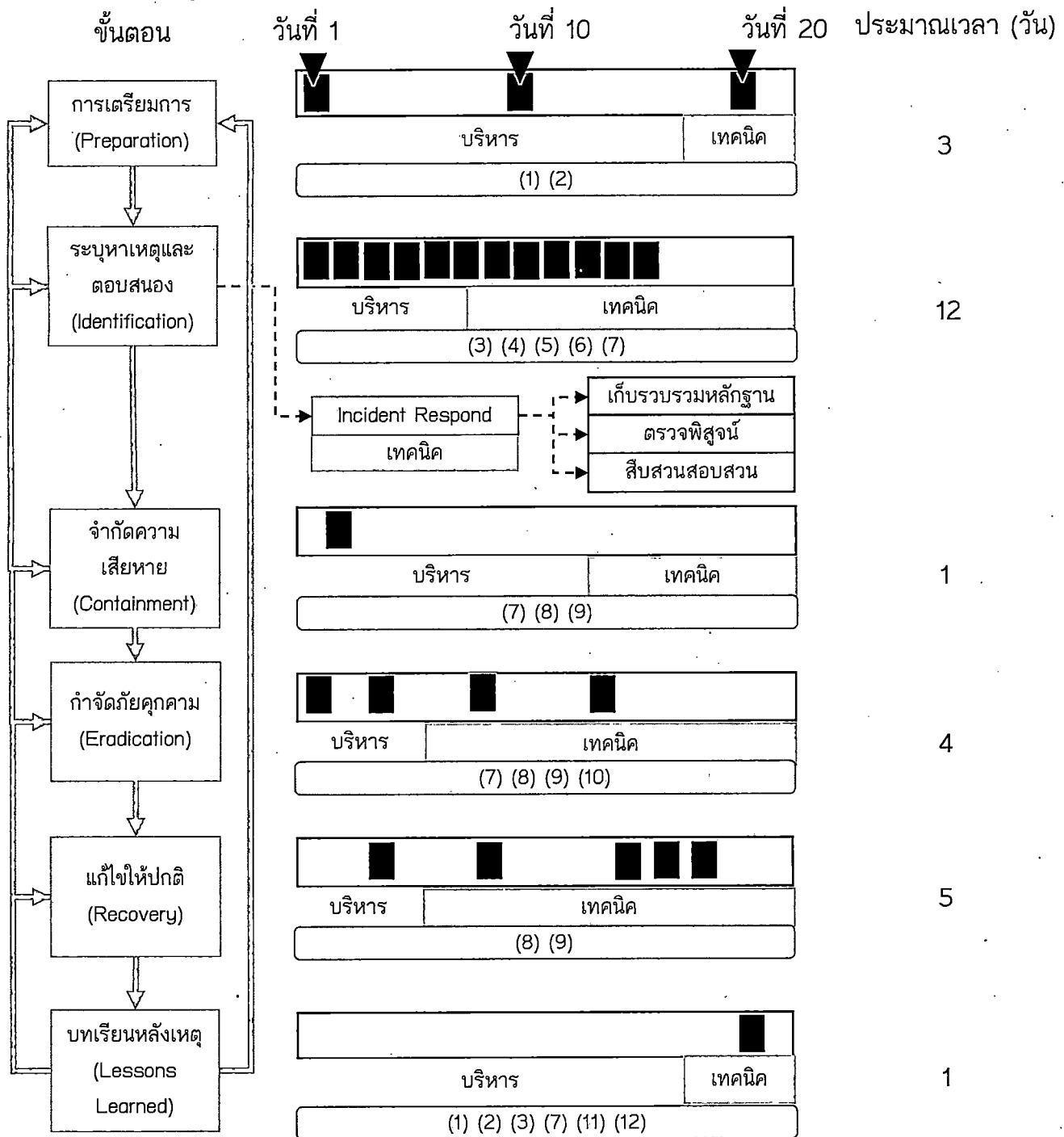
สถานการณ์/เหตุการณ์

หน่วยงานที่ประสบเหตุ

สกมช.



บทบาทของ สกมช. การสนับสนุนการดำเนินวิธีรับมือภัยคุกคามไซเบอร์
(Incident Handling) ร่วมกับหน่วยงานที่ประสบเหตุ
กรณี Spade Ransomware โจมตีระบบคอมพิวเตอร์โรงพยาบาลของรัฐ



ทักษะ/เทคนิคทางอาชีพที่ใช้ในแต่ละขั้นตอน

- (1) Information Systems Security Manager
- (2) Information Technology (IT) Director
- (3) Incident Analyst
- (4) Computer Forensic Analyst
- (5) Computer Crime Investigator
- (6) Incident Responder
- (7) Blue Team Technician
- (8) Systems Administrator
- (9) Network Administrator
- (10) Intrusion Detection System Administrator
- (11) Information Manager
- (12) Information Security Manager