ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

โดยที่คณะรัฐมนตรีได้มีมติเมื่อวันที่ ๒๐ กันยายน ๒๕๖๕ เห็นชอบนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ ซึ่งเป็นการจัดทำนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) นั้น

อาศัยอำนาจตามความในมาตรา ๙ (๑) (๒) และ (๓) และมาตรา ๔๓ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และตามคำสั่งสำนักนายกรัฐมนตรี ที่ ๒๓๙/๒๕๖๓ เรื่อง มอบหมายและมอบอำนาจให้รองนายกรัฐมนตรี และรัฐมนตรีประจำสำนักนายกรัฐมนตรีปฏิบัติหน้าที่ประธานกรรมการในคณะกรรมการต่าง ๆ ตามกฎหมาย และระเบียบสำนักนายกรัฐมนตรีและตามมติคณะรัฐมนตรีข้างต้น จึงออกประกาศแจ้งการใช้นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) เพื่อเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติ และเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ ซึ่งสอดคล้องกับยุทธศาสตร์ชาติด้านความมั่นคงแผนย่อย การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง ซึ่งมีเป้าหมายของแนวทางพัฒนาคือปัญหาความมั่นคงที่มีอยู่ในปัจจุบัน (ความมั่นคงทางไซเบอร์) ได้รับการแก้ไขจนไม่ส่งผลกระทบต่อการบริหารและพัฒนาประเทศ ดังมีสาระสำคัญตามที่แนบท้ายประกาศนี้

ทั้งนี้ ประกาศฉบับนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๑๓ พฤศจิกายน พ.ศ. ๒๕๖๕
พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี ปฏิบัติหน้าที่
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

นโยบายและแผนปฏิบัติการ ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

นโยบายและแผนปฏิบัติการ

ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ส่วนที่ ๑ บทสรุปผู้บริหาร

นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕-๒๕๗๐ ฉบับนี้ เป็นการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มาตรา ๙ (๑) บัญญัติให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจ เสนอนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมและสนับสนุนการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๒ และมาตรา ๔๓ ต่อคณะรัฐมนตรีเพื่อให้ความเห็นชอบ

นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ใช้เป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย การพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมที่ครอบคลุมในทุกมิติ และเพื่อใช้เป็นกรอบแนวทางการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

มาตรา ๙ (๓) บัญญัติให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจ จัดทำแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์เสนอต่อคณะรัฐมนตรีสำหรับเป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ โดยแผนดังกล่าวจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติ และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

ส่วนที่ ๒ ความสอดคล้องกับแผน ๓ ระดับ ตามนัยยะของมติคณะรัฐมนตรี เมื่อวันที่ ๔ ธันวาคม ๒๕๖๐

๒.๑ ยุทธศาสตร์ชาติ (แผนระดับที่ ๑)

๒.๑.๑ ยุทธศาสตร์ชาติ ด้านความมั่นคง

เป้าหมายที่ ๓ กองทัพ หน่วยงานด้านความมั่นคง ภาครัฐ ภาคเอกชนและภาคประชาชน มีความพร้อมในการป้องกันและแก้ไขปัญหาความมั่นคง

เป้าหมายที่ ๔ ประเทศไทยมีบทบาทด้านความมั่นคงเป็นที่ชื่นชมและได้รับการยอมรับโดยประชาคมระหว่างประเทศ

เป้าหมายที่ ๕ การบริหารจัดการความมั่นคงมีผลสำเร็จที่เป็นรูปธรรมอย่างมีประสิทธิภาพ

๒.๑.๒ ประเด็นยุทธศาสตร์

ข้อ ๔.๒ การป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

ข้อ ๔.๒.๑ การแก้ไขปัญหาความมั่นคงในปัจจุบัน

ข้อ ๔.๒.๒ การติดตาม เฝ้าระวัง ป้องกัน และแก้ไขปัญหาที่อาจอุบัติขึ้นใหม่

๒.๒ แผนระดับที่ ๒

๒.๒.๑ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ

ประเด็นยุทธศาสตร์ด้านความมั่นคง

ข้อ ๓.๒ แผนย่อยการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

๒.๒.๒ แผนปฏิรูปประเทศด้านสื่อสารมวลชน เทคโนโลยีสารสนเทศ

ประเด็นยุทธศาสตร์แผนปฏิรูปประเทศด้านสื่อสารมวลชน เทคโนโลยีสารสนเทศ

ข้อ ๕.๕ การปฏิรูปการบริหารจัดการความปลอดภัยไซเบอร์ /กิจการอวกาศและระบบและเครื่องมือด้านการสื่อสารมวลชนและโทรคมนาคมเพื่อสนับสนุนภารกิจการป้องกันบรรเทาสาธารณภัย ภายใต้กิจกรรมที่ ๑ การปกป้องคุ้มครองและรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญด้านสารสนเทศของประเทศ

๒.๒.๓ แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ ๑๒

ยุทธศาสตร์ที่ ๕ การเสริมสร้างความมั่นคงแห่งชาติเพื่อการพัฒนาประเทศสู่ความมั่งคั่งและยั่งยืน

แนวทางการพัฒนาที่ ๓.๒ การพัฒนาเสริมสร้างศักยภาพการป้องกันประเทศ เพื่อเตรียมความพร้อมในการรับมือภัยคุกคาม ทั้งการทหารและภัยคุกคามอื่น ๆ

ยุทธศาสตร์ที่ ๗ การพัฒนาโครงสร้างพื้นฐานและระบบโลจิสติกส์

แนวทางการพัฒนาที่ ๓.๕ การพัฒนาเศรษฐกิจดิจิทัล

๒.๒.๔ นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๒ – ๒๕๖๕)

นโยบายที่ ๑๐ เสริมสร้างความมั่นคงปลอดภัยไซเบอร์ รองรับวัตถุประสงค์ ๓.๔.๕ เพื่อพัฒนาศักยภาพของภาครัฐ และส่งเสริมบทบาทและความเข้มแข็งของทุกภาคส่วนในการรับมือกับภัยคุกคามทุกรูปแบบที่กระทบกับความมั่นคง

แผนที่ ๑๕ การป้องกันและแก้ไขความมั่นคงทางไซเบอร์

๒.๓ แผนระดับที่ ๓ ที่เกี่ยวข้อง

๒.๓.๑ นโยบายและแผนระดับชาติว่าด้วยการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (พ.ศ ๒๕๖๑ – ๒๕๘๐)

ยุทธศาสตร์ที่ ๖ สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

แผนงาน ข้อ ๓ สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัลและการทำธุรกรรมออนไลน์

๒.๓.๒ แผนปฏิบัติการด้านดิจิทัลเพื่อเศรษฐกิจและสังคมระยะ ๕ ปี (พ.ศ. ๒๕๖๒ - ๒๕๖๕)

เป้าหมายที่ ๕ สร้างความเชื่อมั่น

ประเด็นขับเคลื่อน ๕.๑ การเสริมสร้างความมั่นคงปลอดภัยไซเบอร์

ประเด็นขับเคลื่อน ๕.๒ ขับเคลื่อนการพัฒนากฎหมายและมาตรฐานดิจิทัล

เป้าหมายที่ ๖ พัฒนากำลังคนดิจิทัล

ประเด็นขับเคลื่อน ๖.๑ การพัฒนากำลังคนและประชาชนสู่ยุคดิจิทัล

๒.๓.๓ ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ ๒๕๖๐ - ๒๕๖๕)

ประเด็นยุทธศาสตร์ที่ ๑ เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

ประเด็นยุทธศาสตร์ที่ ๒ ปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๓ ปกป้องผลประโยชน์และความมั่นคงของชาติให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

ประเด็นยุทธศาสตร์ที่ ๔ เสริมสร้างระบบเศรษฐกิจดิจิทัล

ประเด็นยุทธศาสตร์ที่ ๕ สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประเด็นยุทธศาสตร์ที่ ๖ เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม

ประเด็นยุทธศาสตร์ที่ ๗ ส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

ประเด็นยุทธศาสตร์ที่ ๘ ส่งเสริมบทบาทที่สร้างสรรค์ของไทยในความร่วมมือเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคและระดับนานาชาติ

๒.๓.๔ แผนเตรียมพร้อมแห่งชาติ (พ.ศ. ๒๕๖๐-๒๕๖๕)

ยุทธศาสตร์ที่ ๓ การเสริมสร้างความร่วมมือ การเตรียมพร้อมรับมือภัยคุกคามกับต่างประเทศ

กลยุทธ์ ข้อ ๔ เสริมสร้างความสัมพันธ์และความร่วมมือการเตรียมพร้อมด้านวิกฤตการณ์ความมั่นคงกับต่างประเทศ อาทิ การก่อวินาศกรรม การก่อการร้าย ภัยความมั่นคงทางไซเบอร์ ภัยความมั่นคงทางอวกาศ โรคติดต่ออุบัติใหม่ ให้สอดคล้องกับนโยบายรัฐบาล นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ และยุทธศาสตร์ความมั่นคงเฉพาะด้านที่เกี่ยวข้อง

ส่วนที่ ๓ สาระสำคัญของ นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕-๒๕๗๐

๓.๑ การประเมินสถานการณ์ ปัญหา ความจำเป็นของนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕-๒๕๗๐

ปัจจุบันเทคโนโลยีดิจิทัลมีบทบาทสำคัญในการเป็นเครื่องมืออำนวยความสะดวกแก่การดำรงชีวิตประจำวัน โดยรายงานของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union :ITU) พบว่า ปี พ.ศ. ๒๕๖๑ มีจำนวนผู้ใช้อินเทอร์เน็ต คิดเป็นร้อยละ ๕๑ ของประชากรทั่วโลก โดยคาดว่า ภายในปี พ.ศ. ๒๕๖๖ จะมีจำนวนผู้ใช้งานอินเทอร์เน็ต เพิ่มขึ้นถึงร้อยละ ๗๐ ของประชากรทั่วโลก

ผลสำรวจพฤติกรรมผู้ใช้งานอินเทอร์เน็ตในประเทศไทยปี พ.ศ. ๒๕๖๑ โดยสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (สพธอ.) พบว่า ประเทศไทยก้าวสู่สังคมดิจิทัลอย่างเต็มรูปแบบแล้ว ซึ่งค่าเฉลี่ยของการใช้งานอินเทอร์เน็ตของคนไทยเติบโตเพิ่มขึ้นมากกว่าปีที่ผ่านมาถึง ๓ เท่า ทั้งนี้ ความก้าวหน้าทางเทคโนโลยีดิจิทัล โดยเฉพาะอย่างยิ่งการใช้อินเทอร์เน็ตมาพร้อมกับความท้าทายและภัยคุกคามทางไซเบอร์ซึ่งมีหลากหลายรูปแบบ ไม่ว่าจะเป็นการเผยแพร่ ข้อมูลที่ไม่เป็นจริง

การพยายามบุกรุกเข้าระบบ การโจมตีสภาพการใช้งานของระบบ การพัฒนาโปรแกรมที่ไม่พึงประสงค์ และการสร้างหน้าเว็บไซต์ปลอมเพื่อหลอกลวงหาผลประโยชน์ เป็นต้น อันก่อให้เกิดความเสียหายแก่ประเทศชาติ ภาคธุรกิจ และปัจเจกบุคคล

จากข้อมูลสถิติภัยคุกคามทางไซเบอร์ของไทย ปี พ.ศ. ๒๕๖๑ รวบรวมโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) พบว่าความพยายามบุกรุกเข้าระบบสารสนเทศ (Intrusion Attempts) เป็นภัยคุกคามไซเบอร์ อันดับ ๑ ของประเทศไทย คิดเป็นสัดส่วนร้อยละ ๔๓ จากจำนวนภัยคุกคาม ทั้งหมด ๒,๕๒๐ เหตุการณ์

นอกจากนี้ ผลจากการสำรวจความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ ในปี พ.ศ. ๒๕๕๙ และ พ.ศ. ๒๕๖๑ ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) เพื่อวิเคราะห์ถึงสถานการณ์ ปัญหา อุปสรรค และการรับมือกับภัยคุกคามไซเบอร์ของประเทศไทย โดยมีหลักการพิจารณา ๑) การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ ๒) การปกป้องดูแลอุปกรณ์สารสนเทศ ๓) ความสามารถในการตรวจพบเหตุภัยคุกคาม ๔) การรับมือภัยคุกคาม และ ๕) การกู้คืนระบบหลังเกิดเหตุ พบว่า การรับมือภัยคุกคามไซเบอร์ของหน่วยงานภาครัฐและภาคเอกชนมากกว่า ๕๐๐ หน่วยงาน มีค่าเฉลี่ยในระดับต่ำ

จากสถานการณ์ภัยคุกคามไซเบอร์ข้างต้นที่เกิดขึ้นอย่างรวดเร็วและรุนแรงขึ้นทุกปี การขาดแคลนบุคลากรที่ปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อันส่งผลต่อความสามารถในการดำเนินการ จนส่งผลให้ถูกโจมตีทางไซเบอร์และส่งผลต่อเศรษฐกิจของประเทศไทยอย่างมหาศาล ถึงแม้ว่าจะมีการลงทุนในการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เพิ่มสูงขึ้น แต่ในประเทศไทยเองยังขาดแคลนบุคลากร และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ ทำให้ต้องพึ่งพาบุคลากรและผลิตภัณฑ์จากต่างประเทศ ดังนั้น จึงมีความจำเป็นต้องกำหนดนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ในการเสริมสร้างศักยภาพในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตลอดจนตอบสนองต่อเหตุภัยคุกคามและฟื้นฟูระบบให้กลับคืนสู่สภาวะปกติอย่างทันท่วงที

๓.๒ สาระสำคัญของ นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕ - ๒๕๗๐

นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับสมบูรณ์นี้ ได้กำหนดวิสัยทัศน์การรักษาความมั่นคงปลอดภัยไซเบอร์ คือ **“บริการที่สำคัญของประเทศไทยมีความมั่นคงปลอดภัยไซเบอร์ เพื่อความยั่งยืนทางเศรษฐกิจและสังคม”**

นโยบายและแผนปฏิบัติการเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๕ – ๒๕๗๐ เป็นแผนแม่บทในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติ และในสถานการณ์ที่อาจจะเกิดหรือเกิดภัยคุกคามทางไซเบอร์ ซึ่งสอดคล้องกับนโยบายยุทธศาสตร์และแผนระดับชาติ และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

เพื่อให้บรรลุวิสัยทัศน์และเป้าหมายการขับเคลื่อนยุทธศาสตร์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงได้กำหนดยุทธศาสตร์การดำเนินงาน ๔ ยุทธศาสตร์ ดังนี้

๓.๒.๑ ยุทธศาสตร์ที่ ๑ : สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Capacity)

วัตถุประสงค์

เพื่อเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยบูรณาการ-บุคลากร องค์ความรู้ และเทคโนโลยี นำไปสู่การพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมของประเทศ

เป้าหมาย

๑. พัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์เพื่อรองรับความต้องการของประเทศ

๒. ส่งเสริมให้บุคลากรทุกภาคส่วนมีความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

๓. ส่งเสริมให้เกิดการมีส่วนร่วมในการสร้างความแข็งแกร่งด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

๔. ส่งเสริมการพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นนวัตกรรมของประเทศ

กลยุทธ์ที่ ๑.๑ เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์

๑. พัฒนาหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ทั้งภาคทฤษฎีและภาคปฏิบัติ เป็นสาขาเฉพาะทางในระดับอุดมศึกษา รองรับความต้องการของภาคอุตสาหกรรมที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒. พัฒนาทักษะและฝึกอบรมบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในระดับผู้บริหารและผู้ปฏิบัติงาน

ตัวชี้วัดของกลยุทธ์

๑. มีหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ทั้งภาคทฤษฎีและภาคปฏิบัติ เป็นสาขาเฉพาะทางในระดับอุดมศึกษา รองรับความต้องการของภาคอุตสาหกรรมที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ไม่น้อยกว่า ๕ สถาบัน

๒. บุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งในระดับผู้บริหารและผู้ปฏิบัติงานไม่น้อยกว่าร้อยละ ๘๐ ได้รับการพัฒนาความรู้และทักษะ

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการพัฒนากรอบความสามารถและโปรแกรมการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ ส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญในระดับชาติและนานาชาติ

๒. โครงการยกระดับวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ให้เป็นที่ยอมรับ

๓. โครงการพัฒนาบุคลากรทางไซเบอร์โดยส่งเสริมให้มีสถาบันการศึกษามีหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์เฉพาะทาง

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการพัฒนากรอบความสามารถและโปรแกรม	๑) จัดทำกรอบความสามารถและโปรแกรมการฝึกอบรมด้านความปลอดภัยทางไซเบอร์สำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ และสำหรับผู้ที่ไม่ใช่	**หลัก:** สกมช. **รอง:** สพร. สพธอ.

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
การฝึกอบรมด้านความปลอดภัยทางไซเบอร์ ส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญในระดับชาติและนานาชาติ	ไอที (non-IT) การออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญ ๒) จัดทำหลักสูตรและเนื้อหาสำหรับตอบสนองกรอบความสามารถและโปรแกรมการฝึกอบรม การออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญ ๓) กำหนดให้ใช้กรอบความสามารถและโปรแกรมการฝึกอบรมด้านความปลอดภัยทางไซเบอร์สำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และสำหรับผู้ที่ไม่ใช่ไอที (non-IT) เป็นส่วนหนึ่งในข้อกำหนดจ้างงาน/เลื่อนตำแหน่ง ๔) เป็นพันธมิตร ให้ทุนส่งเสริมและสนับสนุนให้มีหน่วยงานที่สนับสนุนฝึกอบรมด้านความปลอดภัยทางไซเบอร์สำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และสำหรับผู้ที่ไม่ใช่ไอที (non-IT) การออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญ โดยอาจพิจารณาสิทธิพิเศษทางภาษี และมาตรการส่งเสริมต่าง ๆ เพื่อเพิ่มจำนวนของหน่วยงานสนับสนุน ๕) ส่งเสริม เผยแพร่ จัดอบรม และทุนสนับสนุนอย่างต่อเนื่อง ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	สำนักงาน ก.พ. ดศ. สคช. สดช. สอศ. อว. หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ บก.ทท. สปท. บีโอไอ
๒. โครงการยกระดับวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ยอมรับ	๑) กำหนดแนวทางค่าตอบแทนของวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ให้เหมาะสมและจูงใจ ๒) จัดกิจกรรมส่งเสริม สนับสนุน รวมถึงมีกิจกรรมการแข่งขันอย่างต่อเนื่อง ๓) หารือกับหน่วยงานที่เกี่ยวข้องกำหนดกรอบอัตรากำลังและค่าตอบแทนที่เหมาะสม ๔) เผยแพร่ประชาสัมพันธ์ผู้ที่เป็นต้นแบบและแรงบันดาลใจในสายงาน ๕) ส่งเสริม สนับสนุน ผู้ที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง และเป็นรูปธรรม	**หลัก:** สกมช. **รอง:** สพร. สพธอ. สำนักงาน ก.พ. สคช. อว. สดช. สอศ. สพฐ. ดศ. สำนักงบประมาณ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ บก.ทท. สปท.
๓. โครงการพัฒนาบุคลากรทางไซเบอร์โดยส่งเสริมให้มีสถาบันการศึกษามีหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์เฉพาะทาง	๑) จัดทำกรอบบูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์เฉพาะทางในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับมัธยม ประกาศนียบัตรวิชาชีพ (ปวช.) จนถึงปริญญาเอก ๒) จัดทำหลักสูตรและเนื้อหาทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์เฉพาะทางในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับมัธยม ประกาศนียบัตรวิชาชีพ (ปวช.) จนถึงปริญญาเอก ๓) จัดกิจกรรมส่งเสริม รวมถึงการแข่งขันเพื่อหาบุคลากรที่มีความสามารถในการทำงาน พัฒนาวิจัย และสร้างผลิตภัณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ ๔) ปรับปรุงระเบียบและข้อปฏิบัติในการจ่ายค่าตอบแทนให้เหมาะสมกับผู้ปฏิบัติงานการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีทักษะขั้นสูง ๕) สร้างความร่วมมือระหว่างภาคส่วนต่าง ๆ ในการบูรณาการ ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. สำนักงาน ก.พ. สคช. สดช. สอศ. สพฐ. อว. ดศ. สำนักงบประมาณ หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ บก.ทท. สปท.

กลยุทธ์ที่ ๑.๒ สร้างความตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์

๑. สร้างความตระหนักและการรู้เท่าทัน ด้านความมั่นคงปลอดภัยไซเบอร์

๒. ส่งเสริมให้เกิดการบูรณาการหลักสูตรเกี่ยวกับการตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ ในระบบการศึกษาทุกระดับชั้น

ตัวชี้วัดของกลยุทธ์

๑. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวนไม่น้อยกว่าร้อยละ ๘๐ มีกิจกรรมการสร้างความตระหนักและการรู้เท่าทันด้านความมั่นคงปลอดภัยไซเบอร์ในแต่ละปี

๒. มีการบูรณาการหลักสูตรเกี่ยวกับการตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ ในระบบการศึกษาทุกระดับชั้น

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการบูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์กับทักษะดิจิทัลในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษาจนถึงระดับหลังปริญญา

๒. โครงการสร้างความตระหนักรู้ระดับชาติสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) และหลากหลายรูปแบบ

๓. โครงการพัฒนาหลักปฏิบัติ (Code of practices) เพื่อความมั่นคงปลอดภัยของอุปกรณ์และผลิตภัณฑ์ที่เชื่อมต่ออินเทอร์เน็ต

๔. โครงการให้ความรู้ประชาชนเกี่ยวกับกฎหมาย กฎระเบียบ ความเสี่ยงของอาชญากรรมไซเบอร์ และมาตรการป้องกัน

๕. โครงการฝึกซ้อมเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ของประเทศ กิจกรรมการจัดการฝึกและทดสอบแผนเผชิญเหตุ ในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติในระดับประเทศ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการบูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์กับทักษะดิจิทัลในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษาจนถึงระดับหลังปริญญา	๑) จัดทำกรอบบูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์กับทักษะดิจิทัลในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษาจนถึงระดับหลังปริญญา ๒) จัดทำหลักสูตรและเนื้อหาทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์กับทักษะดิจิทัลในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษาจนถึงระดับหลังปริญญา ๓) จัดกิจกรรมส่งเสริม รวมถึงการแข่งขันเพื่อหาบุคลากรที่มีความสามารถในการทำงาน พัฒนาวิจัย และสร้างผลิตภัณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ ๔) ปรับปรุงระเบียบและข้อปฏิบัติในการพิจารณาการเลื่อนตำแหน่งหรือค่าตอบแทนต้องผ่านเกณฑ์ทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์	**หลัก:** สกมช. **รอง:** สพร. สพธอ. สำนักงาน ก.พ. สคช. สดช. สอศ. สพฐ. อว. ดศ. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๕) สร้างความร่วมมือระหว่างภาคส่วนต่าง ๆ ในการบูรณาการ ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๒. โครงการสร้างความตระหนักรู้ระดับชาติสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) และหลากหลายรูปแบบ	๑) จัดทำกรอบโปรแกรมสร้างความตระหนักรู้ระดับชาติด้วยแคมเปญที่กำหนดเป้าหมายสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) ๒) จัดทำหลักสูตรและเนื้อหาโปรแกรมสร้างความตระหนักรู้ที่กำหนดเป้าหมายสำหรับกลุ่มเป้าหมายที่แตกต่างกัน ๓) จัดกิจกรรมส่งเสริม เผยแพร่โปรแกรมสร้างความตระหนักรู้ระดับชาติ ผ่านช่องทางที่หลากหลายตรงกับกลุ่มเป้าหมาย เช่น ละคร โฆษณา การ์ตูน เพลง หรือสื่ออื่น ๆ รวมถึงการให้รางวัลผู้ร่วมกิจกรรม ๔) พัฒนาแพลตฟอร์มในการเผยแพร่โปรแกรมสร้างความตระหนักรู้ระดับชาติ ๕) สนับสนุนการมีส่วนร่วม โดยอาจพิจารณาสิทธิพิเศษทางภาษี และมาตรการส่งเสริมต่าง ๆ เพื่อเพิ่มจำนวนของหน่วยงานสนับสนุน ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. สดช. สอศ. สพฐ. อว. ดศ. หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๓. โครงการพัฒนาหลักปฏิบัติ (Code of practices) เพื่อความมั่นคงปลอดภัยของอุปกรณ์และผลิตภัณฑ์ที่เชื่อมต่ออินเทอร์เน็ต	๑) จัดทำหลักปฏิบัติ (Code of practices) เพื่อความมั่นคงปลอดภัยของอุปกรณ์และผลิตภัณฑ์ที่เชื่อมต่ออินเทอร์เน็ต ๒) สนับสนุน เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๓) สนับสนุนการมีส่วนร่วม โดยอาจพิจารณาสิทธิพิเศษทางภาษี และมาตรการส่งเสริมต่าง ๆ เพื่อเพิ่มจำนวนของหน่วยงานสนับสนุน ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สพร. สพธอ. กพ. สคช. สดช. สอศ. สพฐ. อว. ดศ. สทป. บก.ทท. บีโอไอ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๔. โครงการให้ความรู้ประชาชนเกี่ยวกับกฎหมาย กฎระเบียบ ความเสี่ยงของอาชญากรรมไซเบอร์ และมาตรการป้องกัน	๑) พิจารณากฎหมาย กฎระเบียบ ความเสี่ยงของอาชญากรรมไซเบอร์ และมาตรการป้องกันแต่ละปีที่จะให้ความรู้กับประชาชน ๒) จัดทำ ปรับปรุง หรือสร้างแนวทางในการให้ความรู้ประชาชนเกี่ยวกับกฎหมาย กฎระเบียบ ความเสี่ยงของอาชญากรรมไซเบอร์ และมาตรการป้องกัน ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตร. สพร. สพธอ. สำนักงาน ก.พ. สคช. สดช. สอศ. สพฐ. อว. ดศ.
๕.โครงการฝึกซ้อมเพื่อการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ของประเทศ กิจกรรมการจัดการฝึกและทดสอบแผนเผชิญเหตุ ในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับวิกฤติในประเทศ	๑) จัดการประชุมวางแผนการฝึก (Exercise planning) ๒) จัดการประชุมเพื่อจัดทำสถานการณ์และโจทย์ฝึก (Exercise Development) ๓) จัดการฝึกเตรียมการ (Pre-exercise/Academic) ๔) จัดการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ในรูปแบบการฝึกฝ่ายเสนาธิการ (Staff Exercise : Staff-Ex) หรือ การฝึกปัญหาที่บังคับการ (Command Post Exercise : CPX) หรือการฝึกภาคสนาม (Field Training Exercise : FTX) ๕) จัดทำรายงานสรุปผลการฝึก	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กลยุทธ์ที่ ๑.๓ ส่งเสริมการวิจัยและพัฒนาและนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์

๑. ส่งเสริมการศึกษา วิจัย พัฒนาและสร้างนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์

๒. ส่งเสริมความร่วมมือด้านวิจัยและพัฒนา ระหว่างหน่วยงานวิจัยในประเทศและต่างประเทศ

๓. ส่งเสริมการลงทุนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. ส่งเสริมการพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นนวัตกรรม และสามารถต่อยอดเชิงพาณิชย์ได้

ตัวชี้วัดของกลยุทธ์

๑. มีการศึกษา วิจัย พัฒนาและสร้างนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ปีละไม่น้อยกว่า ๑ ฉบับ

๒. มีความร่วมมือด้านวิจัยและพัฒนา ระหว่างหน่วยงานวิจัยในประเทศและต่างประเทศ อย่างน้อย ๑๐ หน่วยงาน

๓. มีการลงทุนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของจำนวนหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่น้อยกว่าร้อยละ ๕๐

๔. มีผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมสามารถต่อยอดเชิงพาณิชย์ได้

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการส่งเสริมและสนับสนุน ให้ทุน และจัดทำแพลตฟอร์มการวิจัยและพัฒนา นวัตกรรม วิทยาศาสตร์และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. โครงการส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ

๓. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมการจัดตั้งห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Lab)

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการส่งเสริมและสนับสนุน ให้ทุน และจัดทำแพลต - ฟอร์มการวิจัยและพัฒนา นวัตกรรม วิทยาศาสตร์และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์	๑) จัดตั้งศูนย์แห่งความเป็นเลิศ (Centers of excellence) หรือศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ ๒) มีการเผยแพร่สมุดปกขาว บอกทิศทางและแนวทางในการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยของประเทศเป็นรายปี และใช้กำหนดทิศทางในการพัฒนาและให้ทุนสนับสนุน ๓) ส่งเสริมการทำงานร่วมกัน (Collaboration) รูปแบบการระดมทุน ๔) พัฒนาฟอรัมหรือแพลตฟอร์มการวิจัยและพัฒนาสำหรับความร่วมมือระหว่างภาครัฐและเอกชน ๕) เผยแพร่กลยุทธ์วิทยาศาสตร์และเทคโนโลยีไซเบอร์ ๖) ให้ทุนและสนับสนุนการวิจัยวิทยาศาสตร์และเทคโนโลยีไซเบอร์ ๗) สนับสนุนประชาชนชาวไทย นักศึกษา นักวิจัย เพื่อเพิ่มจำนวนชาวไทยที่มีความเชี่ยวชาญด้านไซเบอร์	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สพร. สพธอ. สำนักงาน ก.พ. สดช. สอศ. สพฐ. อว. ดศ. สทป. บก.ทท. บีโอไอ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๘) สนับสนุนงบประมาณในการวิจัยการระบุและจัดหาโซลูชั่นที่เป็นนวัตกรรมสำหรับปัญหาเร่งด่วนที่สุดบางประการในด้านความมั่นคงปลอดภัยไซเบอร์ ๙) สนับสนุนการมีส่วนร่วม โดยอาจพิจารณาสิทธิพิเศษทางภาษี และมาตรการส่งเสริมต่าง ๆ เพื่อเพิ่มจำนวนของหน่วยงานสนับสนุน ๑๐)กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๒. โครงการส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชันและผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ	๑) จัดทำนโยบายและแนวทางในการส่งเสริมการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ ๒) ให้ความรู้และความร่วมมือกับสตาร์ทอัพด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย โดยร่วมมือกับนักวิจัย มหาวิทยาลัย บริษัทชั้นนำทั้งในและต่างประเทศ ๓) สร้างแบรนด์และความน่าเชื่อถือของโซลูชันและผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ ๔) ส่งเสริมการใช้โซลูชันและผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ โดยให้สิทธิพิเศษและการสนับสนุนในด้านต่าง ๆ ๕) สนับสนุนการมีส่วนร่วม โดยอาจพิจารณาสิทธิพิเศษทางภาษี และมาตรการส่งเสริมต่าง ๆ เพื่อเพิ่มจำนวนของหน่วยงานสนับสนุน ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สพร. สพธอ. สำนักงาน ก.พ. สคช. สดช. สอศ. สพฐ. อว. ดศ. สทป. บก.ทท. บีโอไอ
๓. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมการจัดตั้งห้องปฏิบัติการความมั่นคงปลอดภัย	๑) จัดทำกรอบแนวคิดในการดำเนินงาน และแผนการดำเนินงานในโครงการฯ พร้อมทั้งอธิบายรายละเอียด ระยะเวลา และผู้รับผิดชอบในโครงการ ๒) จัดซื้อเครื่องมือเพิ่มเติม และติดตั้งประจำศูนย์ NCSA ๓) ทดสอบการใช้งานระบบ และปรับแต่งให้ตรงกับความต้องการ ๔) จัดอบรมเกี่ยวกับการใช้งานให้กับเจ้าหน้าที่ที่เกี่ยวข้องให้ใช้เครื่องมือได้อย่างมีประสิทธิภาพมากขึ้น ๕) ทดสอบวิธีการเจาะระบบ (Penetration Test)	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
ไซเบอร์ (Cyber Security Lab)	กลุ่มเป้าหมาย ไม่น้อยกว่า ๑๕ หน่วยงาน เพื่อรายงานช่องโหว่ให้กับหน่วยงานรับทราบและดำเนินการป้องกัน และทำการตรวจพิสูจน์หลักฐานทางดิจิทัล ให้กับหน่วยงานที่ได้รับการโจมตีทางไซเบอร์ ไม่น้อยกว่า ๑๐ หน่วยงาน	

๓.๒.๒ ยุทธศาสตร์ที่ ๒ : บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)

วัตถุประสงค์

เพื่อบูรณาการความร่วมมือในการเตรียมความพร้อมสำหรับการรับมือภัยคุกคามทางไซเบอร์ และการฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้อย่างรวดเร็วกับทุกภาคส่วนทั้งภายในประเทศและระหว่างประเทศ

เป้าหมาย

๑. มีการประสานความร่วมมือทั้งภาครัฐและภาคเอกชนภายในประเทศเพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์และการฟื้นคืนสู่สภาพปกติ

๒. มีการประสานความร่วมมือระหว่างประเทศ เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์และการฟื้นคืนสู่สภาพปกติ

กลยุทธ์ที่ ๒.๑ ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและภาคเอกชน

๑. ระบุถึงการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสีย เพื่อสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน

๒. กำหนดโครงสร้างการกำกับดูแลที่ชัดเจน และกำหนดกลไกที่ทำหน้าที่สร้างความร่วมมือและประสานงานระหว่างหน่วยงานภาครัฐ และภาคเอกชน

๓. สร้างความร่วมมือระหว่างหน่วยงานภาครัฐ

๔. รักษาสมดุลระหว่างความมั่นคงปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล

๕. สนับสนุนการพัฒนาศักยภาพบุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดของกลยุทธ์

๑. มีกิจกรรมเพื่อสร้างความร่วมมือระหว่างหน่วยงานภาครัฐ ภาคเอกชน ปีละไม่น้อยกว่า ๓ กิจกรรม

๒. มีโครงสร้างการกำกับดูแลที่ชัดเจน มีกลไกความร่วมมือและประสานงานระหว่างหน่วยงานภาครัฐ ระหว่างภาครัฐและภาคเอกชน และระหว่างภาคเอกชน

๓. มีความร่วมมือระหว่างหน่วยงานภาครัฐ ปีละไม่น้อยกว่า ๓ กิจกรรม

๔. มีแนวทางความร่วมมือระหว่างหน่วยงานความมั่นคงปลอดภัยทางไซเบอร์และหน่วยงานการคุ้มครองข้อมูลส่วนบุคคล

๕. บุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้รับการพัฒนาศักยภาพ ปีละไม่น้อยกว่า ๑ ครั้ง

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อระบุและตอบสนองต่อปัญหาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว

๒. โครงการประสานหน่วยงานภาคธุรกิจ มุ่งเน้นไปที่ชุมชนธุรกิจ เพื่อรวมความมั่นคงปลอดภัยไซเบอร์เข้ากับการจัดการความเสี่ยงขององค์กร

๓. โครงการสนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับชาติ (เช่น กรอบการดำเนินการร่วมกันในการต่อต้านอาชญากรรมไซเบอร์เฉพาะทาง การดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ เช่น ตำรวจ และเจ้าหน้าที่ฝ่ายตุลาการ ผู้เชี่ยวชาญนิติวิทยาศาสตร์)

๔. โครงการการเป็นพันธมิตรกับหน่วยงานคุ้มครองข้อมูลส่วนบุคคล สำหรับการจัดแนวทางการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและการปฏิบัติตามข้อกำหนดในการปกป้องข้อมูลส่วนบุคคล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อระบุและตอบสนองต่อปัญหาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว	๑) ส่งเสริมและสนับสนุนการกำหนดกรอบความร่วมมือระหว่างภาครัฐและเอกชนและความร่วมมือระหว่างประเทศเพื่อระบุและตอบสนองต่อปัญหาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว ๒) จัดทำแนวทางตามกรอบการปฏิบัติการ ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. ตร. หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๒. โครงการประสานหน่วยงานภาคธุรกิจ มุ่งเน้นไปที่ชุมชนธุรกิจ เพื่อรวมความมั่นคงปลอดภัยไซเบอร์ เข้ากับการจัดการความเสี่ยงขององค์กร	๑) กำหนดแนวทางในการสร้างความร่วมมือกับชุมชนธุรกิจ เพื่อรวมความปลอดภัยทางไซเบอร์เข้ากับการจัดการความเสี่ยงขององค์กร ๒) จัดทำหรือปรับปรุงกฎหมาย กฎระเบียบที่เกี่ยวข้อง ๓) สนับสนุน เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. ดศ. สดช. สศด. หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๓. โครงการสนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับชาติ (เช่น กรอบการดำเนินการร่วมกันในการต่อต้านอาชญากรรมไซเบอร์เฉพาะทาง พัฒนาการฝึกอบรมเฉพาะสำหรับการดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ เช่น ตำรวจและเจ้าหน้าที่ฝ่ายตุลาการ ผู้เชี่ยวชาญนิติวิทยาศาสตร์)	๑) กำหนดกรอบการดำเนินการร่วมกันในการต่อต้านอาชญากรรมไซเบอร์เฉพาะทาง พัฒนาการฝึกอบรมเฉพาะสำหรับการดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ ๒) จัดทำแนวทางตามกรอบการปฏิบัติการ ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. ตร. สำนักงานอัยการสูงสุด (อส.) หน่วยงานควบคุมหรือกำกับดูแล ยธ. กห. บก. ทท.
๔. โครงการการเป็นพันธมิตรกับหน่วยงานคุ้มครองข้อมูลส่วนบุคคล สำหรับการจัดแนวทางการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและการปฏิบัติตามข้อกำหนดในการปกป้องข้อมูลส่วนบุคคล	๑) จัดทำกรอบในการทำงานร่วมกันกับหน่วยงานคุ้มครองข้อมูลส่วนบุคคลสำหรับการจัดแนวทางการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยและการปฏิบัติตามข้อกำหนดในการปกป้องข้อมูลส่วนบุคคล ๒) จัดทำหรือปรับปรุงกฎหมาย กฎระเบียบที่เกี่ยวข้อง ๓) สนับสนุน เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. ดศ. หน่วยงานควบคุมหรือกำกับดูแลคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

กลยุทธ์ที่ ๒.๒ ประสานความร่วมมือระหว่างประเทศเพื่อรับมือภัยคุกคาม

๑. กำหนดให้การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นสำคัญในการกำหนดนโยบายด้านการต่างประเทศ

๒. มีส่วนร่วมในเวทีการประชุมระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์

๓. สร้างความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศในทุกมิติ

๔. พัฒนายุทธศาสตร์ของประเทศให้สอดคล้องตามแนวปฏิบัติสากล

๕. สนับสนุนการพัฒนาศักยภาพบุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายระหว่างประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่นที่เกี่ยวข้อง เพื่อให้สามารถปฏิบัติงานร่วมกับหน่วยงานที่เกี่ยวข้องในระดับนานาชาติได้อย่างมีประสิทธิภาพ

ตัวชี้วัดของกลยุทธ์

๑. มีการกำหนดให้การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นนโยบายด้านการต่างประเทศ

๒. มีการเข้าร่วมประชุมระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์ในทุกกรอบความร่วมมือระหว่างประเทศ

๓. มีความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศในทุกมิติ อาทิ การบังคับใช้กฎหมาย การแลกเปลี่ยนข้อมูลภัยคุกคามไซเบอร์ เป็นต้น

๔. มีการพัฒนายุทธศาสตร์ของประเทศให้สอดคล้องตามแนวปฏิบัติสากล

๕. มีกิจกรรมเพื่อพัฒนาศักยภาพบุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายระหว่างประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่นที่เกี่ยวข้อง ได้รับการพัฒนาศักยภาพ เพื่อให้สามารถปฏิบัติงานร่วมกับหน่วยงานที่เกี่ยวข้องในระดับนานาชาติได้อย่างมีประสิทธิภาพ ปีละไม่น้อยกว่า ๑ ครั้ง

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการสนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับนานาชาติ

๒. โครงการส่งเสริมและสนับสนุนการแลกเปลี่ยนด้าน Cyber Norms และกฎหมายที่เกี่ยวข้อง

๓. โครงการส่งเสริมและสนับสนุนความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติ เพื่อสร้างศักยภาพด้านไซเบอร์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการสนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับนานาชาติ	๑) ส่งเสริมและสนับสนุนการกำหนดกรอบการดำเนินการร่วมกันในการต่อต้านอาชญากรรมไซเบอร์เฉพาะทาง พัฒนาการฝึกอบรมเฉพาะสำหรับการดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ ในระดับนานาชาติ ๒) จัดทำแนวทางตามกรอบการปฏิบัติการ	**หลัก:** สกมช. **รอง:** สพร. สพธอ. ตร. กต.

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๒. โครงการส่งเสริมและสนับสนุนการแลกเปลี่ยนด้าน Cyber Norms และกฎหมายที่เกี่ยวข้อง	๑) กำหนดกรอบสนับสนุนการแลกเปลี่ยนด้าน Cyber Norms และกฎหมายที่เกี่ยวข้อง ๒) จัดทำแนวทางสนับสนุนการแลกเปลี่ยนด้าน Cyber Norms และกฎหมายที่เกี่ยวข้อง ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. กต. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๓. โครงการส่งเสริมและสนับสนุนความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติเพื่อสร้างศักยภาพด้านไซเบอร์	๑) กำหนดกรอบส่งเสริมความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติเพื่อสร้างศักยภาพด้านไซเบอร์ ๒) จัดทำแนวทางส่งเสริมความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติเพื่อสร้างศักยภาพด้านไซเบอร์ ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. กต. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๒.๓ ยุทธศาสตร์ที่ ๓ : สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Resilience)

วัตถุประสงค์

เพื่อส่งเสริมบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์ และสามารถฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้

เป้าหมาย

๑. มีการกำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒. มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓. มีการปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ

กลยุทธ์ที่ ๓.๑ กำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)

๑. ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยระบุถึงประเภทของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกำหนดมาตรการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๒. กำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ

๓. ส่งเสริมและสนับสนุนหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design)

๔. ส่งเสริมและสนับสนุนให้บุคลากรทุกระดับมีความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดของกลยุทธ์

๑. มีการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกำหนดมาตรการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ครบทุกด้านตามประกาศของ สกมช.

๒. มีการกำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)

๓. มีการส่งเสริมและสนับสนุนหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design) สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)

๔. มีการส่งเสริมให้บุคลากรทุกระดับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) มีความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์ ไม่น้อยกว่าร้อยละ ๘๐

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการพัฒนาหลักปฏิบัติ (Code of practices) และจรรยาบรรณ (Code of conduct) ที่เป็นมาตรฐานและขั้นตอนการตรวจสอบและติดตามการปฏิบัติตาม (Compliance)

๒. โครงการส่งเสริมและสนับสนุนหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design)

๓. โครงการส่งเสริมและสนับสนุนการสร้างความตระหนักรู้โดยเฉพาะที่กำหนดเป้าหมาย CII (ผู้บริหารสูงสุด และพนักงาน)

๔. โครงการขับเคลื่อนแผน ยุทธศาสตร์ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กิจกรรมพัฒนาขีดความสามารถ กระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการพัฒนาหลักปฏิบัติ (Code of practices) และ จรรยาบรรณ (Code of conduct) นโยบายและแนวทางที่เป็นมาตรฐานและขั้นตอนการตรวจสอบและติดตามการปฏิบัติตาม (Compliance)	๑) จัดทำพัฒนาหลักปฏิบัติ (Code of practices) และจรรยาบรรณ (Code of conduct) นโยบายและแนวทาง (Policies and Guideline) ที่เป็นมาตรฐานและขั้นตอนการตรวจสอบและติดตามการปฏิบัติตาม (Compliance) ๒) ส่วนของ Policies and Guideline ควรมีการสร้างความร่วมมือกับหน่วยงานด้านมาตรฐาน เช่น ISO หรือ NIST รวมถึงหน่วยงานภายใน เช่น ETDA เพื่อให้นโยบายและแนวปฏิบัติ มีความน่าเชื่อถือและไม่เกิดความสับสนต่อผู้ปฏิบัติ (CII) ๓) กำหนดแนวทางการใช้งานหลักปฏิบัติในแต่ละภาคส่วน ๔) ช่วยเหลือสำหรับธุรกิจในการปฏิบัติตาม ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๒. โครงการส่งเสริมและสนับสนุนหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design)	๑) จัดทำหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design) ๒) กำหนดระเบียบข้อบังคับ นโยบายและแนวทางที่เกี่ยวข้อง ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๓. โครงการส่งเสริมและสนับสนุนการสร้างความตระหนักรู้โดยเฉพาะที่กำหนดเป้าหมาย CII (ผู้บริหารสูงสุดและพนักงาน)	๑) จัดทำกรอบโปรแกรมการสร้างความตระหนักรู้โดยเฉพาะที่กำหนดเป้าหมาย CII (ผู้บริหารสูงสุดและพนักงาน) ๒) กำหนดระเบียบข้อบังคับ นโยบายและแนวทางที่เกี่ยวข้อง โดยกำหนดให้เป็นส่วนหนึ่งของภาระหน้าที่ในการปฏิบัติ การเลื่อนตำแหน่ง ๓) เผยแพร่ประชาสัมพันธ์ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. ก.พ. หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๔. โครงการขับเคลื่อนแผนยุทธศาสตร์นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์	๑) ศึกษาเพื่อทบทวนหลักสูตรเพื่อการพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากล ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวน 2 หลักสูตร ประกอบด้วย หลักสูตรผู้นำการปฏิบัติ (Lead	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลและหน่วยงานโครงสร้างพื้นฐาน

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
กิจกรรมพัฒนาขีดความสามารถกระบวนการปฏิบัติงานด้านไซเบอร์ตามมาตรฐานสากลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	Implementor) และหลักสูตรผู้นำตรวจสอบ (Lead Auditor) ๒) จัดประชุมรับฟังความคิดเห็นจากผู้ที่มีส่วนเกี่ยวข้อง (Focus Group) เนื้อหาหลักสูตรผู้นำการปฏิบัติ (Lead Implementor) และหลักสูตรผู้นำตรวจสอบ (Lead Auditor) ๓) จัดประชุมประชาพิจารณ์ต่อ เนื้อหาหลักสูตรผู้นำการปฏิบัติ (Lead Implementor) และหลักสูตรผู้นำตรวจสอบ (Lead Auditor) ๔) จัดอบรมเชิงปฏิบัติการหลักสูตรผู้นำการปฏิบัติ (Lead Implementor) และหลักสูตรผู้นำตรวจสอบ(Lead Auditor) ๕) จัดทำเว็บไซต์สำหรับการสอนหลักสูตรผู้นำการปฏิบัติ (Lead Implementor) และหลักสูตรผู้นำตรวจสอบ (Lead Auditor)ผ่านระบบออนไลน์	สำคัญทางสารสนเทศ

กลยุทธ์ที่ ๓.๒ กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑. กำหนดวิธีการบริหารจัดการความเสี่ยงเพื่อปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒. พัฒนากลไกแนวทางการกำกับดูแลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และพิจารณากำหนดให้ ข้อมูลและบริการคลาวด์ (Data & Cloud Computing) เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ต้องมีการกำกับดูแลในระยะต่อไป

๓. พัฒนากฎหมาย กฎระเบียบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ทันสมัย

ตัวชี้วัดของกลยุทธ์

๑. มีวิธีการบริหารจัดการความเสี่ยงเพื่อปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒. มีกลไกและแนวทางการกำกับดูแลของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓. มีกฎหมาย กฎระเบียบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ทันสมัย

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการกฎระเบียบและข้อบังคับที่สนับสนุนทำให้เกิดความมั่นคงปลอดภัยไซเบอร์

๒. โครงการพัฒนากรอบการทำงานที่ถูกต้องตามกฎหมายสำหรับ CII (แนวทางและการควบคุมกำกับดูแล)

๓. โครงการพัฒนากลไกในการบูรณาการเหตุการณ์ความเสี่ยงทางไซเบอร์ สถานะการดำเนินการของผู้ดำเนินการ CII และกฎหมาย/แนวโน้มระหว่างประเทศเพื่อปรับปรุงแก้ไขหรือเกิดผลทางกฎหมายเพิ่มเติมอย่างทันท่วงที

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการกฎระเบียบและข้อบังคับที่สนับสนุนทำให้เกิดความมั่นคงปลอดภัยไซเบอร์	๑) การทบทวนกฎระเบียบและข้อบังคับที่สนับสนุนความมั่นคงปลอดภัยไซเบอร์ เช่น การปฏิบัติงานระหว่างหน่วยงาน ขอบเขตอำนาจหน้าที่และการประสานงาน การแบ่งปันข้อมูลข่าวสาร การรักษาความลับและข้อมูลส่วนบุคคล การคุ้มครองการปฏิบัติงานของเจ้าหน้าที่ การเก็บรวบรวม การใช้ และดูแลรักษาหลักฐานดิจิทัลที่ใช้ในชั้นศาล เป็นต้น ๒) จัดทำหรือปรับปรุงระเบียบและข้อบังคับที่สนับสนุนความมั่นคงปลอดภัยไซเบอร์ ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** ยธ. สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล
๒. โครงการพัฒนากรอบการทำงานที่ถูกต้องตามกฎหมายสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (แนวทาง และการควบคุมกำกับดูแล)	๑) กำหนดแนวทางการบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหลักการควบคุมหรือกำกับดูแล (Governance) และการบริหารจัดการความเสี่ยง ๒) พัฒนารูปแบบการกำกับดูแลของภาครัฐและภาระความรับผิดชอบ (Adopt a governance model with clear responsibilities) ของหน่วยงานภาครัฐและผู้มีส่วนเกี่ยวข้องในการปกป้องคุ้มครองโครงสร้างพื้นฐานสำคัญ (Critical infrastructures: CIs) และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CIIs) ๓) กำหนดระเบียบข้อบังคับที่เกี่ยวข้อง ๔) การสนับสนุนการร่วมลงทุนระหว่างภาครัฐและภาคเอกชน (Establish public-private partnerships) การสร้างแรงจูงใจในทุกภาคส่วน (Utilize a wide range of market levers)	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๕) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๓. โครงการพัฒนากลไกในการบูรณาการเหตุการณ์ความเสี่ยงทางไซเบอร์ สถานะการดำเนิน การของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกฎหมาย/แนวโน้มระหว่างประเทศเพื่อปรับปรุงแก้ไขหรือเกิดผลทางกฎหมายเพิ่มเติมอย่างทันท่วงที	๑) จัดทำกลไกในการบูรณาการเหตุการณ์ความเสี่ยงทางไซเบอร์ สถานะการดำเนินการของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกฎหมาย/แนวโน้มระหว่างประเทศเพื่อปรับปรุงแก้ไขหรือเกิดผลทางกฎหมายเพิ่มเติมอย่างทันท่วงที ๒) กำหนดระเบียบข้อบังคับที่เกี่ยวข้อง ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** ยธ. กต. สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล

กลยุทธ์ที่ ๓.๓ ปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ

๑. กำหนดให้หน่วยงานภาครัฐปฏิบัติตามนโยบายมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ

๒. กำหนดให้มีการประเมินความเสี่ยงจากการใช้เทคโนโลยีเพื่อให้เกิดความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน

๓. กำหนดมุมมองการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกัน

๔. เตรียมความพร้อมด้านบุคลากร ข้อมูล เทคโนโลยี และกระบวนการเพื่อรับมือภัยคุกคามไซเบอร์สมัยใหม่

ตัวชี้วัดของกลยุทธ์

๑. มีการกำหนดให้หน่วยงานภาครัฐปฏิบัติตามนโยบาย มาตรฐานการรักษา ความมั่นคงปลอดภัยขั้นต่ำ เพิ่มขึ้นปีละไม่น้อยกว่าร้อยละ ๑๐

๒. มีการกำหนดให้มีการประเมินความเสี่ยงจากการใช้เทคโนโลยีเพื่อให้เกิดความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน เพิ่มขึ้นปีละไม่น้อยกว่าร้อยละ ๑๐

๓. มีกิจกรรมการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกัน อย่างน้อยปีละไม่ต่ำกว่า ๑ ครั้ง

๔. มีกิจกรรมที่เกี่ยวกับการเตรียมความพร้อมด้านบุคลากร ข้อมูล เทคโนโลยี และกระบวนการเพื่อรับมือภัยคุกคามภัยไซเบอร์สมัยใหม่ ปีละไม่น้อยกว่า ๑ กิจกรรม

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการส่งเสริมและสนับสนุนการนำเทคโนโลยีมาใช้เพื่อให้เกิดความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน (Security by default)

๒. โครงการพัฒนาและบังคับใช้มาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับบริการภาครัฐ (เช่น ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่รวมอยู่ในสัญญาด้านเทคโนโลยีสารสนเทศของรัฐบาล)

๓. โครงการสร้างการจัดการแบบบองค์รวมของเครือข่ายที่ดำเนินการโดยหน่วยงานของรัฐ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการส่งเสริมและสนับสนุนการนำเทคโนโลยีมาใช้เพื่อให้เกิดความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน (Security by default)	๑) จัดทำแนวปฏิบัติ "ความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน (Security by default)" ๒) จัดทำมาตรการสนับสนุนให้ผู้ให้บริการฮาร์ดแวร์และซอฟต์แวร์ให้ปฏิบัติตามแนวทางปฏิบัติ "ความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน (Security by default)" ๓) สำรวจวิธีกระตุ้นตลาดด้วยการให้คะแนนความมั่นคงปลอดภัยสำหรับผลิตภัณฑ์ใหม่ ๔) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๒. โครงการพัฒนาและบังคับใช้มาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับบริการภาครัฐ (เช่น ข้อกำหนดมาตรฐาน	๑) จัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับบริการภาครัฐ เช่น ข้อกำหนดมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่รวมอยู่ในสัญญาด้านไอทีของรัฐบาล แนวทางและเกณฑ์ในการพิจารณาความเสี่ยงในการเลือกผู้ให้บริการ	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
ความมั่นคงปลอดภัยไซเบอร์ที่รวมอยู่ในสัญญาด้านไอทีของรัฐบาล)	และผลิตภัณฑ์, Backdoor Policy, การพิจารณาความเสี่ยงจาก Vendor Lock in ๒) กำหนดระเบียบข้อบังคับที่เกี่ยวข้อง ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๓. โครงการสร้างการจัดการแบบองค์รวมของเครือข่ายที่ดำเนินการโดยหน่วยงานของรัฐ	๑) กำหนดกรอบการจัดการแบบองค์รวมของเครือข่ายที่ดำเนินการโดยหน่วยงานของรัฐ เช่น ให้มีหน่วยงานกลางที่รับผิดชอบของแต่ละกรม มีการเชื่อมโยงขอบเขต อำนาจหน้าที่ และการประสานงานระหว่างกรมไปยังกระทรวง และการเชื่อมโยงของแต่ละกระทรวง การดำเนินการโดยหน่วยงานกลางหรือการกระจายอำนาจ และประสานการทำงานร่วมกัน ๒) จัดทำแพลตฟอร์มการจัดการแบบองค์รวมของเครือข่ายที่ดำเนินการโดยหน่วยงานของรัฐ ๓) ปรับปรุงและสนับสนุนการเข้าถึงผู้เชี่ยวชาญด้านไซเบอร์ในหน่วยงานของรัฐ ๔) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๒.๔ ยุทธศาสตร์ที่ ๔ : สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน (Standard)

วัตถุประสงค์

มุ่งสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

เป้าหมายและตัวชี้วัด

๑. มีการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์แบบบูรณาการในระดับชาติ

๒. มีหน่วยงานหลักและหน่วยงานรองที่มีคุณภาพและมาตรฐาน สามารถทำงานร่วมกันแบบบูรณาการได้

๓. มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

๔. มีการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

๕. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศมีมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เข้มแข็ง

กลยุทธ์ที่ ๔.๑ เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๑. พิจารณาศึกษาและทบทวนนโยบาย กฎหมาย และขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบัน เพื่อกำหนดแนวทางการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

๒. กำหนดกลไกการขับเคลื่อนยุทธศาสตร์ กระบวนการตัดสินใจ การแบ่งหน้าที่ความรับผิดชอบ การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง แนวทางการดำเนินการและการติดตามประเมินผลการปฏิบัติงาน

๓. ส่งเสริมบุคลากร (People) กระบวนการ (Process) และเทคโนโลยี (Technology) ให้มีการพัฒนาศักยภาพ คุณภาพ และมาตรฐาน เพื่อสร้างความเชื่อมั่นให้กับผู้มีส่วนได้เสีย และนำมาตรฐานและแนวปฏิบัติที่ดีมาใช้ในการปฏิบัติงาน โดยอาจดำเนินการเพื่อให้ได้รับใบรับรอง (Certification) และการรับรอง (Accreditation) ในส่วนของการปฏิบัติงานที่สำคัญ

๔. พัฒนาแผนรองรับสถานการณ์ฉุกเฉินด้านไซเบอร์ เพื่อใช้ในการรับมือและฟื้นฟูบริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยจัดตั้งทีมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security Incident Response Team: CSIRT) ตลอดจนการฝึกซ้อมแผนรับมือปัญหาความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดของกลยุทธ์

๑. มีการทบทวนนโยบาย กฎหมาย และขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบัน เพื่อกำหนดแนวทางการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ

๒. มีแนวทางการติดตามประเมินผลการปฏิบัติงาน

๓.ส่งเสริมให้มีการพัฒนาศักยภาพบุคลากร (People) กระบวนการ (Process) และเทคโนโลยี (Technology) ให้มีคุณภาพตามมาตรฐาน เพิ่มขึ้นปีละไม่น้อยกว่าร้อยละ ๑๐

๔. มีแผนเตรียมพร้อมด้านการรองรับสถานการณ์ฉุกเฉินด้านไซเบอร์เพื่อใช้ในการรับมือและฟื้นฟูบริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมีการจัดตั้งทีมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ ตลอดจนการฝึกซ้อมแผนรับมือปัญหาความมั่นคงปลอดภัยไซเบอร์ จำนวนไม่น้อยกว่า ๑ แผน

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการส่งเสริมและสนับสนุนการปฏิบัติงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ให้มีคุณภาพและมาตรฐาน

๒. โครงการเพิ่มขีดความสามารถสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

๓. โครงการปรับปรุงกฎหมาย ระเบียบและข้อบังคับในด้านความมั่นคงปลอดภัยไซเบอร์

๔. โครงการผสานรวมการค้นพบภัยคุกคาม การวิเคราะห์ และการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๕. โครงการจัดทำแผนฉุกเฉินสำหรับการจัดการวิกฤตความมั่นคงปลอดภัยไซเบอร์

๖. โครงการจัดระเบียบและดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์

๗. โครงการการสกัดกั้นภัยคุกคามในระดับผู้ให้บริการโทรคมนาคม

๘. โครงการส่งเสริมและสนับสนุนการรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ

๙. โครงการขับเคลื่อนแผน ยุทธศาสตร์ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กิจกรรมยกระดับขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Self-Assessment)

๑๐. โครงการการฝึกซ้อมเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ของประเทศ กิจกรรมการจัดทำแผนเผชิญเหตุด้านไซเบอร์ (National Incident Response Plan)

๑๑. โครงการจัดตั้ง Sectoral CERT และพัฒนาแพลตฟอร์มรักษาความปลอดภัยทางไซเบอร์เพื่อรับมือเหตุฉุกเฉินทางคอมพิวเตอร์สำหรับ Sectoral CERT ของหน่วยงานด้านสาธารณสุข

โครงการ	**แนวทางการดำเนินการ**	**หน่วยงานรับผิดชอบ**
๑. โครงการส่งเสริมและสนับสนุนการปฏิบัติงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ให้มีคุณภาพและมาตรฐาน	๑) การจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) ๒) การพัฒนาระบบสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ๓) การจัดตั้งห้องปฏิบัติการวิเคราะห์ข้อมูลทางเทคนิคสำหรับการทดสอบเจาะระบบ การตรวจพิสูจน์หลักฐาน การทดสอบอุปกรณ์ CERT ของแต่ละภาคส่วนของหน่วยงาน CII (Sector CERT) ศูนย์วิเคราะห์ข่าวกรองทางไซเบอร์ (Cyber	**หลัก:** ดศ. สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล บก.ทท. กห. ตร.

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	Threat Intelligence Fusion Center), อุปกรณ์และเครื่องมือของ CPT (Cyber Protection Team) ๔) การจัดตั้งระบบแผนกช่วยเหลือ (Help Desk) ในศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ๕) การจัดตั้งศูนย์ปฏิบัติการร่วมทางไซเบอร์ของแต่ละหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ๖) นำมาตรฐานและแนวปฏิบัติที่ดีมาใช้ในการปฏิบัติงาน พร้อมทั้งได้รับใบรับรอง (Certification) และการรับรอง (Accreditation) ในส่วนของการปฏิบัติงานที่สำคัญ เช่น ISO/IEC 27001, ISO 22301, ISO/IEC 20000-1, ISO/IEC 38500 เป็นต้น ๗) จัดทำระบบในการกำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่องแบบ real-time ๘) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง ๙) กำหนดหน่วยงานควบคุมหรือกำกับดูแลของแต่ละภาคส่วน (CII Sector) พร้อมทั้งส่งเสริมและสนับสนุนการทำงานของ CII Sector จัดให้หน่วยงานสนับสนุนในระดับภูมิภาค เช่น มหาวิทยาลัย เอกชน สถาบันการศึกษา หน่วยงานที่มีความชำนาญเฉพาะด้าน เป็นต้น เพื่อช่วยเหลือการทำงานของ CII Sector ๑๐) กำกับดูแล ติดตาม ประเมินผล ส่งเสริม และสนับสนุนอย่างต่อเนื่อง	
๒. โครงการเพิ่มขีดความสามารถสำนักงานคณะกรรมการการรักษาความมั่นคง	๑) การสร้างทีมปฏิบัติการป้องกันภัยไซเบอร์ (Cyber Protection Team : CPT) ๒) อบรมเพื่อพัฒนาทักษะทางไซเบอร์สำหรับผู้บริหารและผู้ปฏิบัติงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	**หลัก:** ดศ. สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทาง

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
ปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	๓) การจัดหาระบบฝึกซ้อมในการรับมือภัยคุกคามทางไซเบอร์ ๔) จัดตั้งศูนย์อบรม Cybersecurity Training Center ๕) จัดหาระบบ Cybersecurity Learning Platform ๖) เพิ่มศักยภาพในการกำกับดูแล (Governance) โดยกำหนดให้มีการจัดตั้ง “ประชาคมไซเบอร์แห่งชาติ” โดยมีสมาชิก เป็นผู้แทนหน่วยงานกำกับและหน่วยงานปฏิบัติ จากแต่ละ CII มีวัตถุประสงค์เพื่อให้เกิดการแลกเปลี่ยนองค์ความรู้ และแนวคิดให้เกิดการปฏิบัติตาม แผนปฏิบัติการฯ นโยบายการบริหารจัดการ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ร่วมถึงแนวทางการปฏิบัติอื่น ๆ ที่จะมีตามมาในภายหลัง ๗) การส่งเสริมและสนับสนุนให้มีหน่วยงานพันธมิตรที่สนับสนุนด้านความมั่นคงปลอดภัยเพื่อช่วยเหลือภารกิจต่าง ๆ โดยหน่วยงานพันธมิตรควรมาจากหลากหลายภาคส่วน และหลากหลายภูมิภาค ๘) กำกับดูแล ติดตาม ประเมินผล ส่งเสริม และสนับสนุนอย่างต่อเนื่อง	สารสนเทศ บก.ทท. กห. ตร. สดช. สทป. อว. DEPA
๓. โครงการปรับปรุงกฎหมาย ระเบียบ และข้อ บังคับในด้านความมั่นคงปลอดภัยไซเบอร์	๑) การทบทวนแก้ไข หรือแนวทางในการสร้างกฎหมายในด้านมั่นคงปลอดภัยไซเบอร์ ๒) จัดทำ ปรับปรุง หรือสร้างกฎหมายในด้านมั่นคงปลอดภัยไซเบอร์ ๓) เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดให้เจ้าหน้าที่ของรัฐมีทักษะที่เกี่ยวข้อง ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล ยธ. กห. ตร. สพร. สพธอ.
๔. โครงการผสานรวมการค้นพบภัยคุกคามการวิเคราะห์ และการ	๑) จัดทำกรอบการดำเนินการการผสานรวมการค้นพบภัยคุกคาม ๒) การวิเคราะห์ และการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
ตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	๓) สร้างกลไกการรายงานเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์จากทุกภาคส่วน ๔) การพัฒนาระบบการรายงานเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และการวิเคราะห์และตอบสนองกึ่งอัตโนมัติ หรืออัตโนมัติ ๕) การพัฒนาบุคลากรในการปฏิบัติการวิเคราะห์และการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ๖) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๕. โครงการจัดทำแผนฉุกเฉินสำหรับการจัดการวิกฤตความมั่นคงปลอดภัยไซเบอร์	๑) กำหนดกรอบในการจัดทำแผนฉุกเฉิน (Contingency plans) สำหรับการจัดการวิกฤตความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ เพื่อรองรับการจัดการในสถานการณ์ฉุกเฉินหรือภาวะวิกฤตของประเทศ โดยเฉพาะระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ ควรคำนึงถึงผลการประเมินความเสี่ยงระดับประเทศและระดับภาคส่วนต่าง ๆ ซึ่งสามารถส่งผลกระทบเชื่อมโยงมายังโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศได้ ๒) ส่งเสริมและให้ความรู้ความเข้าใจแก่หน่วยงานที่เกี่ยวข้อง ๓) ทบทวน ปรับปรุงกรอบในการจัดทำแผนฉุกเฉินสำหรับการจัดการวิกฤตความมั่นคงปลอดภัยไซเบอร์ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล สมช. บก.ทท.
๖. โครงการจัดระเบียบและดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์	๑) กำหนดแนวทางในการดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ ๒) ประชาสัมพันธ์และประกาศใช้แนวทางในดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ ๓) ดำเนินการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ระหว่างภาคส่วนต่าง ๆ	**หลัก:** สกมช. **รอง:** สพร. สพธอ. สมช. หน่วยงานควบคุมหรือกำกับดูแล บก.ทท.

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๔) ขยายการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ระดับนานาชาติ ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๗. โครงการการสกัดกั้นภัยคุกคามในระดับผู้ให้บริการโทรคมนาคม	๑) จัดกรอบแนวทางในการสกัดกั้นภัยคุกคามทางไซเบอร์ร่วมกับผู้ให้บริการโทรคมนาคม ๒) จัดทำแนวทางตามกรอบการปฏิบัติการ ๓) สนับสนุน เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ ๔) จัดทำแนวสนับสนุนเมื่อได้รับการร้องขอความร่วมมือจากทางเจ้าหน้าที่ของรัฐเพื่อป้องกันภัยคุกคามทางไซเบอร์ ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** กสทช.
๘. โครงการส่งเสริมและสนับสนุนการรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่นๆ	๑) จัดทำแนวทางในการรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ ผลิตภัณฑ์หรือบริการอื่น ๆ ที่จะนำเข้ามาเชื่อมต่อใช้งาน หรือให้บริการกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical information infrastructure: CII) ต้องมีการพิจารณาด้านความมั่นคงปลอดภัยเข้าไปด้วยในแนวทางและเกณฑ์ในการพิจารณาความเสี่ยงในการเลือกผู้ให้บริการและผลิตภัณฑ์ตลอดวงจรชีวิตของการบริหารจัดการความเสี่ยงจากบุคคลภายนอก (Third Party Risk Management Life Cycle) เช่น นโยบายที่ยืนยันได้ว่าผลิตภัณฑ์หรือบริการนั้นไม่มีการแอบแฝงภัยคุกคามที่ทำงานอยู่ในฉากหลัง (Backdoor Policy) ความเสี่ยงจากการพึ่งพาบุคคลภายนอกรายใดรายหนึ่ง (Third Party/Vendor Locked-in) โดยการพึ่งพาบุคคลภายนอกรายใดรายหนึ่งเป็นหลัก อาจทำให้มีข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยีผู้ให้บริการหรือพันธมิตร และข้อจำกัด	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	ในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง เป็นต้น ซึ่งต้องอาศัยกฎหมาย ระเบียบ ข้อบังคับที่จำเป็นในการบังคับใช้การรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ ๒) ออกกฎหมาย ระเบียบ ข้อบังคับที่จำเป็นในการบังคับใช้การรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ ๓) ให้ความรู้ความเข้าใจในการดำเนินการ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๙. โครงการขับเคลื่อนแผนยุทธศาสตร์นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ กิจกรรมยกระดับขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Self-Assessment)	๑) จัดทำขั้นตอนกิจกรรม การดำเนินงาน และแผนการดำเนินงานในแต่ละขั้นตอน (Action Plan) ๒) ศึกษากรอบแนวคิด เครื่องมือหรือตัวแบบจากข้อมูลทุติยภูมิทั้งในและต่างประเทศที่จะใช้ในการประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Self-Assessment) ๓) จัดทำกรอบแนวคิด เครื่องมือหรือตัวแบบในการประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จะใช้กับหน่วยงานของรัฐที่ไม่ใช่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ๔) จัดประชุมกลุ่มย่อย (Focus group) ผ่านระบบอิเล็กทรอนิกส์ โดยมีผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญของหน่วยงานของรัฐที่ไม่ใช่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานที่เกี่ยวข้อง ๕) จัดทำแบบสอบถามอิเล็กทรอนิกส์เพื่อใช้ในการประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Self-Assessment) ๖) วิเคราะห์ข้อมูลการตรวจสอบความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและจัดทำรายงานผลการประเมินขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	**หลัก:** สกมช. **รอง:** หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑๐. โครงการการฝึกซ้อมเพื่อการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามไซเบอร์ของประเทศ กิจกรรมการจัดทำแผนเผชิญเหตุด้านไซเบอร์ (National Incident Response Plan)	๑) จัดทำแผนการดำเนินงานของกิจกรรมต่าง ๆ ในโครงการฯ พร้อมทั้งอธิบายรายละเอียด ระยะเวลา และผู้รับผิดชอบในแต่ละกิจกรรม ๒) ศึกษา วิเคราะห์ ข้อมูลทั้งจากภายในประเทศและต่างประเทศเพื่อการจัดทำนโยบายและแผน นโยบายการบริหาร และแผนปฏิบัติการ ๓) นำเสนอผลแผนการดำเนินงาน ผลการศึกษาวิเคราะห์ มอบหมายงานให้หน่วยงานที่เกี่ยวข้อง ๔) ดำเนินการงานประชาสัมพันธ์โครงการสู่หน่วยงานภาครัฐ หน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือหน่วยงานที่เกี่ยวข้อง ๕) จัดการอบรมและประชุมเชิงปฏิบัติการเพื่อจัดทำแผนเผชิญเหตุ ในกรณีเกิดเหตุภัยคุกคามทางไซเบอร์ในระดับต่าง ๆ ๖) สรุปผลการดำเนินโครงการ	**หลัก:** สกมช. **รอง:** หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
๑๑. โครงการจัดตั้ง Sectoral CERT และพัฒนาแพลตฟอร์มรักษาความปลอดภัยทางไซเบอร์เพื่อรับมือเหตุฉุกเฉินทางคอมพิวเตอร์สำหรับ Sectoral CERT ของหน่วยงานด้านสาธารณสุข	๑) จัดทำข้อกำหนดและขอบเขตงาน ๒) เก็บรวบรวมข้อมูลและความต้องการจากหน่วยงานโครงการพื้นฐานสำคัญสารสนเทศด้านสาธารณสุขแต่ละหน่วยงาน ๓) ดำเนินการจัดซื้อจัดจ้าง ๔) ดำเนินการติดตั้งระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้กับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและฝึกอบรมบุคลากร ๕) เปิดใช้งานระบบ ๖) สรุปและประเมินผลโครงการ	**หลัก:** สกมช. **รอง:** หน่วยงานโครงการพื้นฐานสำคัญสารสนเทศด้านสาธารณสุข

กลยุทธ์ที่ ๔.๒ ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม

๑.สร้างกลไกการแลกเปลี่ยนข้อมูล ข่าวกรอง และองค์ความรู้ด้านภัยคุกคามทางไซเบอร์

๒. สร้างกลไกการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์

๓.สร้างการมีส่วนร่วมของทุกภาคส่วนในการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์

ตัวชี้วัดของกลยุทธ์

๑. มีการแลกเปลี่ยนข้อมูล ข่าวกรอง และองค์ความรู้ด้านภัยคุกคามทางไซเบอร์ร่วมกัน

๒. มีการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยสามารถระบุสาเหตุและลดเหตุการณ์ภัยคุกคามทางไซเบอร์

๓. มีความร่วมมือของทุกภาคส่วนในการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการสร้างกลไกการแบ่งปันข้อมูลระหว่างภาครัฐและเอกชนและอำนวยความสะดวกในการแบ่งปันข้อมูลความมั่นคงปลอดภัยไซเบอร์

๒. โครงการส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคามระหว่างประเทศ

๓. โครงการพัฒนาแพลตฟอร์มสำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการสร้างกลไกการแบ่งปันข้อมูลระหว่างภาครัฐและเอกชนและอำนวยความสะดวกในการแบ่งปันข้อมูลความมั่นคงปลอดภัยไซเบอร์	๑) สร้างกลไกการแบ่งปันข้อมูลระหว่างภาครัฐและเอกชน ระหว่าง หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ Sector CERT และหน่วยงานความมั่นคง ๒) พัฒนาแพลตฟอร์มสำหรับการรายงานและการแบ่งปันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ข้ามภาคส่วน ๓) พัฒนาระบบแบ่งปันข้อมูลอัตโนมัติ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล กห. ตร.
๒. โครงการส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคามระหว่างประเทศ	๑) สร้างกลไกการแบ่งปันข้อมูลระหว่างภูมิภาคและนานาชาติ และอำนวยความสะดวกในการแบ่งปันข้อมูลความมั่นคงปลอดภัยทางไซเบอร์ การจัดตั้งกลไกการแบ่งปันข้อมูลเพื่อให้สามารถแลกเปลี่ยนข้อมูลข่าวกรองและข้อมูลภัยคุกคามที่ดำเนินการได้ ๒) จัดทำแพลตฟอร์มและระบบสำหรับการแบ่งปันข้อมูลระดับภูมิภาคและนานาชาติ ระบบแบ่งปันข้อมูลอัตโนมัติ (เช่น ระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่แจ้งเตือนได้โดยอัตโนมัติ	**หลัก:** สกมช. **รอง:** สพร. สพธอ. หน่วยงานควบคุมหรือกำกับดูแล กห. ตร.

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	เมื่อเกิดเหตุการณ์หรือการโจมตีทางไซเบอร์) ควบคู่ไปกับแพลตฟอร์มแบ่งปันภัยคุกคามแบบหลายทิศทาง (multi-directional threat-sharing platform) ๓) เพิ่มขีดความสามารถในการแบ่งปันข้อมูลภัยคุกคามระดับภูมิภาคและนานาชาติอย่างต่อเนื่อง ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๓. โครงการพัฒนาแพลตฟอร์มสำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์	๑) จัดทำกรอบแนวคิดในการดำเนินงาน และแผนการดำเนินงานในโครงการฯ พร้อมทั้งอธิบายรายละเอียดระยะเวลา และผู้รับผิดชอบในโครงการ ๒) จัดทำเอกสารเพื่อเป็นแนวทางในการใช้ระบบและเชื่อมต่อ MISP ไปยังหน่วยงานต่าง ๆ - SOP (Standard operating Procedure) for information sharing -หนังสือข้อตกลงในการใช้และเชื่อมต่อระบบ MISP ๓) สร้างความรู้ความเข้าใจถึงการแลกเปลี่ยนข้อมูลตาม SOP ๔) ดำเนินการให้สิทธิ์การเข้าใช้ MISP กลาง ๕) ดำเนินการออกแบบเตรียม Environment ของ สกมช. เพื่อการเชื่อมต่อ ๖) ดำเนินการเชื่อมต่อระบบ MISP เพื่อแลกเปลี่ยนข้อมูลแบบอัตโนมัติอย่างน้อย ๑๐ หน่วยงาน ๗) สรุปผลการดำเนินการ	**หลัก:** สกมช. **รอง:** หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กลยุทธ์ที่ ๔.๓ ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์

๑. สร้างความเชื่อมั่นให้กับทุกภาคส่วนในการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. ยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่ให้บริการที่สำคัญ

๓. ส่งเสริมและสนับสนุนให้เกิดบริการด้านความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดของกลยุทธ์

๑. ทุกภาคส่วนมีความเชื่อมั่นในการรักษาความมั่นคงปลอดภัยไซเบอร์ไม่น้อยกว่าร้อยละ ๕๐

๒. มีการออกกฎหมาย ระเบียบ ข้อบังคับที่จำเป็นในการส่งเสริมให้มีผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. มีจำนวนผู้ให้บริการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพิ่มขึ้นปีละไม่น้อยกว่าร้อยละ ๑๐

โครงการขับเคลื่อนกลยุทธ์

๑. โครงการขยายการสนับสนุนของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ไปยังองค์กรที่ให้บริการที่สำคัญ

๒. โครงการส่งเสริมและสนับสนุนให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยสำหรับที่ให้บริการที่สำคัญ

๓. โครงการขับเคลื่อนแผน ยุทธศาสตร์ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (National CERT)

๕. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมระบบช่วยเหลือ (Help Desk) ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

๖. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมจัดตั้งปฏิบัติการร่วมทางไซเบอร์ (NCSA War room)

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
๑. โครงการขยายการสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ไปยังองค์กรที่ให้บริการที่สำคัญ	๑) จัดทำแนวทางขยายการสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ไปยังองค์กรที่ให้บริการที่สำคัญ ๒) สร้างกลไกขยายการสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ไปยังองค์กรที่ให้บริการที่สำคัญ	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๓) พัฒนาแพลตฟอร์มสำหรับขยายการสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ไปยังองค์กรที่ให้บริการที่สำคัญ ๔) พัฒนาขีดความสามารถในการสนับสนุนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ไปยังองค์กรที่ให้บริการที่สำคัญ ๕) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	
๒. โครงการส่งเสริมและสนับสนุนให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยสำหรับที่ให้บริการที่สำคัญ	๑) จัดทำแนวทางในการส่งเสริมให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยสำหรับองค์กรที่ให้บริการที่สำคัญ ให้สิทธิพิเศษต่าง ๆ ในการดำเนินการกำหนดช่วงเกณฑ์ราคามาตรฐาน ๒) ออกกฎหมาย ระเบียบ ข้อบังคับที่จำเป็นในการส่งเสริมให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยสำหรับองค์กรที่ให้บริการที่สำคัญ ๓) กำกับดูแลการส่งเสริมให้มีผู้ให้บริการด้านความมั่นคงปลอดภัยสำหรับองค์กรที่ให้บริการที่สำคัญ ๔) กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล อส. บีโอไอ
3. โครงการขับเคลื่อนแผน ยุทธศาสตร์ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์	๑) วางแผนการดำเนินงาน จัดทำกรอบแนวคิดในการดำเนินงาน และแผนการดำเนินงานของกิจกรรมต่างๆในโครงการฯ พร้อมทั้งอธิบายรายละเอียด ระยะเวลาและผู้รับผิดชอบในแต่ละกิจกรรม ๒) จัดทำเนื้อหาและรูปแบบการประชาสัมพันธ์การสร้างสื่อการเรียนรู้แบบออนไลน์ ๓) ประชาสัมพันธ์กิจกรรมผ่านสื่อในรูปแบบต่าง ๆ ๔) ดำเนินการจัดประชุมสัมมนาชี้แจงทำความเข้าใจนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ฯ รวมทั้งกฎระเบียบที่เกี่ยวข้อง จำนวน ๔ ครั้ง ครั้งละ ๒ วัน โดยมีผู้เข้าร่วมงานรวม	**หลัก:** สกมช. **รอง:** หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	ไม่น้อยกว่า ๓๐๐ คน ในสถานที่เอกชนและดำเนินการจัดสัมมนาสร้างความรู้ความเข้าใจในรูปแบบออนไลน์ ๕) ติดตามประเมินผลการดำเนินงานโครงการฯ ๖) จัดทำรายงานสรุปผลการดำเนินงานโครงการฯ	
๔. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (National CERT)	๑) ศึกษา วิเคราะห์ จัดทำกรอบแนวคิดในการดำเนินงานการออกแบบและแผนการดำเนินงานในการพัฒนาออกแบบและพัฒนาระบบงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (National CERT) ๒) จัดหาครุภัณฑ์และอุปกรณ์สำหรับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (National CERT) ดำเนินการติดตั้ง และทดสอบระบบและอุปกรณ์ให้พร้อมใช้งานตามข้อกำหนด และจัดทำคู่มือผู้ดูแลระบบและผู้ใช้งาน ๓) ทดสอบการใช้งานระบบ และปรับแต่งให้ตรงกับความต้องการ ๔) ดำเนินการจัดทำรายงานผลการตรวจพบภัยคุกคามความปลอดภัยทางไซเบอร์ของระบบ Threat Hunting Framework (THF) เป็นรายเดือนภายหลังติดตั้งระบบแล้วเสร็จ ๕) จัดให้มีทีมที่ปรึกษาเพื่อสนับสนุนใช้งานระบบให้สามารถใช้งานได้ต่อเนื่องตลอดเวลา ๒๔ ชั่วโมง ใน ๗ วันโดยจะต้องมีผู้บุคคลที่มีความรู้ความสามารถ และมีคุณวุฒิพื้นฐานความรู้ประสบการณ์ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ ผู้ขาย/ผู้รับจ้าง จะต้องส่งบุคลากรประจำศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National CERT) จำนวน ๒ คน ในระยะเวลาปฏิบัติงาน ๑๒ เดือน ในส่วนของอุปกรณ์สำนักงาน เช่น คอมพิวเตอร์ เครื่องพิมพ์ เป็นต้น ผู้ขาย/ผู้รับจ้าง จะต้องเป็นผู้จัดหาให้	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานของรัฐ

โครงการ	แนวทางการดำเนินการ	หน่วยงานรับผิดชอบ
	๖) จัดอบรมเกี่ยวกับการใช้งานให้กับเจ้าหน้าที่ที่เกี่ยวข้อง ๗) เจ้าหน้าที่ดูแล และเฝ้าระวังภัยคุกคามทางไซเบอร์ จัดทำรายงานสรุปภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในแต่ละเดือน จัดทำสรุปแนวโน้มภัยคุกคามทางไซเบอร์รายไตรมาส จัดทำรายงานสรุปผลการดำเนินงานโครงการฯ	
๕. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมระบบช่วยเหลือ (Help Desk) ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	๑) จัดทำกรอบแนวคิดในการดำเนินงาน และแผนการดำเนินงานของกิจกรรมต่าง ๆ ในโครงการฯ พร้อมทั้งอธิบายรายละเอียดระยะเวลา และผู้รับผิดชอบในแต่ละกิจกรรม ๒) ติดตั้งและให้บริการระบบช่วยเหลืองานบริหารการรักษาความมั่นคงปลอดภัยทางไซเบอร์ External Ticketing System ระบบช่วยเหลืองานบริหารการรักษาความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร Internal Ticketing System ระบบรักษาความปลอดภัยสารสนเทศและวิเคราะห์ข้อมูล Data Center ระบบแฟลตฟอร์มการแลกเปลี่ยนข้อมูลข่าวสารภัยคุกคามทางไซเบอร์ ๓) จัดทำรายงานสรุปผลการดำเนินงาน	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานของรัฐ
๖. โครงการจัดตั้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ กิจกรรมจัดตั้งปฏิบัติการร่วมทางไซเบอร์ (NCSA War room)	๑) จัดทำกรอบแนวคิดในการดำเนินงาน และแผนการบำรุงรักษา แก้ไข ซ่อมแซม อุปกรณ์และระบบในโครงการฯพร้อมทั้งอธิบายรายละเอียดระยะเวลาการดำเนินโครงการ ๒) ดำเนินการตรวจสอบระบบและอุปกรณ์ตามวาระปีละ ๔ ครั้ง (ทุก ๓ เดือน) ๓) จัดทำรายงานสรุปผลการบำรุงรักษาในโครงการฯ พร้อมส่งมอบ	**หลัก:** สกมช. **รอง:** หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานของรัฐ

ภาคผนวก

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙(๒) บัญญัติให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) มีหน้าที่และอำนาจ กำหนดนโยบายการบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ จัดทำเพื่อเป็นแนวทางการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตาม (Governance, Risk and Compliance: GRC) สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ใช้หลักการตามแนวทางการปฏิบัติที่ดีที่ใช้กันแพร่หลายทั่วโลก รวมถึงประเทศไทย ซึ่งคือ หลักการกำกับดูแลการบริหารความเสี่ยง และการปฏิบัติตาม (Governance, Risk and Compliance: GRC) ประกอบด้วย ๓ หลักการ ดังนี้

๑. การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)

๑.๑. ต้องจัดโครงสร้างองค์กรให้มีการถ่วงดุล โดยจัดโครงสร้างองค์กร พร้อมกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) ที่มีประสิทธิภาพ โดยมีผู้ที่ทำหน้าที่ควบคุม กำกับ และตรวจสอบที่เป็นอิสระและสามารถทำหน้าที่ได้อย่างมีประสิทธิผล ซึ่งต้องมีการกำหนดหน้าที่ความรับผิดชอบอย่างชัดเจน ทั้งหน่วยงานหรือผู้ก่อให้เกิดความเสี่ยงและควบคุมความเสี่ยงในชั้นแรก (Business Unit หรือ First Line of Defense) มีหน้าที่ดูแลและปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ที่กำหนดไว้ มีการควบคุมภายใน และมีการจัดการความเสี่ยงอย่างเหมาะสม หน่วยงานหรือผู้กำกับภายใน (Second Line of Defense) เช่น หน่วยงานบริหารความเสี่ยง (Risk Management) หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance) และหน่วยงานหรือผู้ตรวจสอบภายใน (Internal Audit หรือ Third Line of Defense) เพื่อส่งเสริมให้มีกลไกการตรวจสอบและถ่วงดุลที่เหมาะสม โดยให้หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศถือปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้องในปัจจุบัน รวมถึงแนวปฏิบัติในเรื่องดังกล่าวที่จะออกโดยหน่วยงานควบคุมหรือกำกับดูแล และจะมีผลบังคับใช้กับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต่อไป

ทั้งนี้ กรณีที่มีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศรวมกับบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้อง การพิจารณาโครงสร้างการกำกับดูแลตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบตาม Three Lines of Defense ให้พิจารณาโดยดูจากภาพรวมทั้งหมดของกลุ่มธุรกิจเดียวกัน

๑.๒. การกำหนดให้มีผู้รับผิดชอบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ หน่วยงานของรัฐต้องจัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่าที่ปฏิบัติหน้าที่ของหน่วยงาน โดยบุคคลดังกล่างต้องเป็นผู้ที่มีความรู้หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือกับภัยคุกคามทางไซเบอร์

ทั้งนี้ผู้บริหารที่ทำหน้าที่ดังกล่าวควรมีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) รวมทั้งควรมีบทบาทหน้าที่และความรับผิดชอบให้หน่วยงานดำเนินการเพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อย ดังนี้

๑) มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด

๒) มีข้อกำหนดด้านความมั่นคงปลอดภัย (security specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT security architecture)

๓) บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ให้สอดรับกับความเสี่ยงที่องค์กรมี และนำเสนอความเสี่ยงดังกล่าวต่อคณะกรรมการหน่วยงานเป็นวาระประจำ

๔) ดูแลและดำเนินการให้หน่วยงานมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

๕) ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านภัยคุกคามทางไซเบอร์

๑.๓ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดให้มีผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer : CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงาน

ทั้งนี้ ผู้บริหารระดับสูงที่ทำหน้าที่ดังกล่าวควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (Authority) เพียงพอในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยสามารถดำเนินการอย่างน้อย ดังนี้

๑) รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและด้านภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด คณะกรรมการของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และคณะกรรมการที่เกี่ยวข้องโดยตรง

๒) ให้ความเห็นด้านภัยคุกคามไซเบอร์และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ คณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee หรือ IT risk committee และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์ที่กระทบต่อหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างมีนัยสำคัญ

๒. การบริหารความเสี่ยง (Risk Management)

๒.๑ ต้องจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เป็นลายลักษณ์อักษร กรอบจะรวมถึง :

(ก) ระบุเกณฑ์ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และระดับความเสี่ยงที่ยอมรับได้ (Risk appetite)

(ข) วิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(ค) การเฝ้าระวังและติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

๒.๒ ต้องเก็บรักษารายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง (Risk register) ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๒.๓ ต้องติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้อย่างสม่ำเสมอ เพื่อให้แน่ใจว่าอยู่ภายใต้เกณฑ์ระดับความเสี่ยงที่ยอมรับได้ที่ระบุไว้ในข้อ ๒.๑ (ก)

๓. นโยบาย และแนวปฏิบัติ (Policies and Guidelines)

๓.๑ ต้องกำหนด และอนุมัตินโยบาย มาตรฐาน และแนวทางในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการป้องกันบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จากภัยคุกคามทางไซเบอร์ นโยบาย มาตรฐาน และแนวปฏิบัติจะต้อง :

(ก) สอดคล้องกับหลักประมวลแนวทางปฏิบัตินี้ ข้อกำหนดการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วน และนโยบาย มาตรฐาน และทิศทางการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับภูมิภาค หรือระดับประเทศ

(ข) เผยแพร่และสื่อสารไปยังบุคลากรและบุคคลภายนอกทุกคนที่ทำหน้าที่หรือสามารถเข้าถึงบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๒ ต้องทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติกับสภาพแวดล้อมการปฏิบัติการไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และภูมิทัศน์ภัยคุกคามทางไซเบอร์ในปัจจุบันอย่างน้อยปีละหนึ่งครั้งโดยนับถัดจากวันที่การทบทวนครั้งสุดท้าย หรือวันที่มีผลบังคับใช้ของนโยบาย มาตรฐาน หรือแนวปฏิบัติแต่ละข้อ

ทั้งนี้ นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนี้มีผลบังคับใช้ภายในหนึ่ง (๑) ปี นับถัดจากวันที่ประกาศ

อภิธานศัพท์

คำศัพท์	ความหมาย
การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)	มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ
ภัยคุกคามทางไซเบอร์ (Cyber threat)	การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง
ไซเบอร์ (Cyber)	ข้อมูลและการสื่อสารที่เกิดจากการให้บริการ หรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียม และระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป
หน่วยงานของรัฐ (Government agency)	ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ
เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident)	เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์
โครงสร้างพื้นฐานสำคัญ (Critical Infrastructure : CI)	บรรดาหน่วยงาน หรือองค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กรซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงาน หรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรนั้นมีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศหรือต่อสาธารณชน

คำศัพท์	ความหมาย
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)	คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical information infrastructure operator)	หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มาตรา ๔๙ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีดังนี้ (๑) ด้านความมั่นคงของรัฐ (๒) ด้านบริการภาครัฐที่สำคัญ (๓) ด้านการเงินการธนาคาร (๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม (๕) ด้านการขนส่งและโลจิสติกส์ (๖) ด้านพลังงานและสาธารณูปโภค (๗) ด้านสาธารณสุข (๘) ด้านอื่นตามที่คณะกรรมการประกาศกำหนดเพิ่มเติม
หน่วยงานควบคุมหรือกำกับดูแล (Regulator)	หน่วยงานของรัฐ หน่วยงานเอกชน หรือ บุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ผลิตภัณฑ์มวลรวมของประเทศ (Gross Domestic Product: GDP)	มูลค่าตลาดของสินค้าและบริการขั้นสุดท้ายที่ผลิตในประเทศในช่วงเวลาหนึ่ง โดยไม่คำนึงว่าผลผลิตนั้นจะเป็นผลผลิตที่ได้จากทรัพยากรภายในหรือภายนอกประเทศ คิดค้นโดย Simon Kuznets นักเศรษฐศาสตร์ชาวรัสเซีย ซึ่งผลิตภัณฑ์มวลรวมในประเทศสามารถใช้เป็นตัวบ่งชี้ถึงมาตรฐานการครองชีพของประชากรในประเทศ
แพลตฟอร์ม (Platform)	ระบบโปรแกรมคอมพิวเตอร์ที่สามารถขยายขีดความสามารถอย่างไม่จำกัด มีการพัฒนาฟังก์ชั่นหรือโมดูลใหม่ๆ มาต่อยอดอยู่ตลอดเวลา เกิดนวัตกรรมใหม่ ๆ เสมอ และสามารถนำไปต่อเชื่อมกับระบบอื่นได้ แพลตฟอร์มไม่ได้จำกัดอยู่แค่ซอฟต์แวร์ แต่ยังรวมไปถึงเว็บไซต์ หรือบริการที่คนอื่นสามารถเขียนโปรแกรมมาต่อเชื่อมหรือดึงข้อมูลได้โดยอัตโนมัติ

คำศัพท์	ความหมาย
ปัญญาประดิษฐ์ (Artificial Intelligence: AI)	ศาสตร์แขนงหนึ่งของวิทยาศาสตร์คอมพิวเตอร์ ที่เกี่ยวข้องกับวิธีการทำให้คอมพิวเตอร์มีความสามารถคล้ายมนุษย์หรือเลียนแบบพฤติกรรมมนุษย์ โดยเฉพาะความสามารถในการคิดเองได้ หรือมีปัญญา ซึ่งปัญญานี้มนุษย์เป็นผู้สร้างให้คอมพิวเตอร์ จึงเรียกว่าปัญญาประดิษฐ์ มุมมองต่อ AI ที่แต่ละคนมีอาจไม่เหมือนกัน ขึ้นอยู่กับว่าเราต้องการความฉลาดโดยคำนึงถึงพฤติกรรมที่มีต่อสิ่งแวดล้อมหรือคำนึงการคิดได้ของผลผลิต AI
ดัชนีความมั่นคงปลอดภัยไซเบอร์โลก (Global Cybersecurity Index : GCI)	ดัชนีชี้วัดระดับของการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ จัดทำโดยสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ดำเนินการร่วมกับสถาบัน ABI Research (Allied Business Intelligence) ซึ่งมีวัตถุประสงค์เพื่อสร้างแรงจูงใจให้แต่ละประเทศตระหนักถึงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยมีเป้าหมายสูงสุดที่ต้องการทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นวัฒนธรรมของโลกและหลอมรวมให้อยู่ในแก่นของเทคโนโลยีสารสนเทศและการสื่อสาร
ทีมรับมือกับสถานการณ์ฉุกเฉินที่เกี่ยวกับคอมพิวเตอร์ (Computer emergency response team: CERT)	CERT หรือ Computer Emergency Response Team เป็นเครื่องหมายการค้าจดทะเบียนของ CERT Coordination Cente (CERT/CC) หมายถึงหน่วยงานรับมือเหตุภัยคุกคามที่อยู่ภายใต้สถาบันวิศวกรรมซอฟต์แวร์ (Software Engineering Institute – SEI) แห่งมหาวิทยาลัย Carnegie Mellon ในสหรัฐอเมริกา และเนื่องจาก CERT เป็นเครื่องหมายการค้าจดทะเบียน ดังนั้น ศูนย์ที่ทำหน้าที่ประสานและรับมือเหตุภัยคุกคามด้านความมั่นคงทางไซเบอร์ที่จัดตั้งขึ้นใหม่ และต้องการใช้ชื่อที่มีคำว่า CERT จะต้องยื่นขอใบอนุญาตเสียก่อน เช่น ประเทศไทย มี Thai CERT
ทีมรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security Incident Response Team: CSIRT) หรือทีมรับมือสถานการณ์ที่เกี่ยวกับคอมพิวเตอร์ (Computer incident response teams: CIRT)	ศูนย์ประสานการรับมือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ที่สามารถรับมือและแก้ไขเหตุภัยคุกคาม ซึ่งประกอบด้วยบุคลากรที่มีความรู้และทักษะในการรับมือเหตุภัยคุกคาม ให้ความช่วยเหลือผู้รับบริการในการฟื้นตัวจากการเจาะระบบ นอกจากนี้ในการดำเนินการเชิงรุก CSIRT สามารถให้บริการตรวจสอบและประเมินช่องโหว่ของระบบ

คำศัพท์	ความหมาย
	สารสนเทศและความเสี่ยงต่าง ๆ รวมทั้งสร้างความตระหนักและให้ความรู้แก่ผู้เกี่ยวข้องในการพัฒนาและปรับปรุงการบริการเพื่อให้เกิดความมั่นคงปลอดภัยไซเบอร์