นโยบายและแผนความมั่นคงที่ ๑๐
การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์

๑. จุดมุ่งเน้น

ประเทศไทยสามารถเพิ่มประสิทธิภาพการป้องกันการโจมตีทางไซเบอร์ การยกระดับมาตรฐานรักษาความมั่นคงปลอดภัยไซเบอร์ และลดการก่ออาชญากรรมทางไซเบอร์

๒. ความเชื่อมโยงกับยุทธศาสตร์ชาติ และ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ

๒.๑ ยุทธศาสตร์ชาติด้านความมั่นคง

เป้าหมาย บ้านเมืองมีความมั่นคงในทุกมิติและทุกระดับ

๒.๒ แผนแม่บทภายใต้ยุทธศาสตร์ชาติ

- **ประเด็นความมั่นคง**

แผนย่อยที่ ๒ แผนย่อยการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

เป้าหมาย ปัญหาความมั่นคงที่มีอยู่ในปัจจุบัน (เช่น ปัญหายาเสพติด ความมั่นคงทางไซเบอร์ การค้ามนุษย์ ฯลฯ) ได้รับการแก้ไขจนไม่ส่งผลกระทบต่อการบริหารและพัฒนาประเทศ

๓. เป้าหมาย ผลสัมฤทธิ์ และตัวชี้วัด

<u>เป้าหมาย</u> ประเทศไทยมีความพร้อมต่อการป้องกัน รับมือความเสี่ยงกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ ทั้งการป้องกันการโจมตีทางไซเบอร์และอาชญากรรมทางไซเบอร์

ผลสัมฤทธิ์ หน่วยงานระดับชาติ กลุ่มภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระดับหน่วยงานมีความพร้อมและมาตรการและแนวทางปฏิบัติในการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เท่าทันเหตุการณ์สอดคล้องกับมาตรฐานสากล รวมถึงมีกลไกและแนวทางในการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ และการพัฒนาการสืบสวนสอบสวนอาชญากรรมทางไซเบอร์

ตัวชี้วัดที่ ๑ การพัฒนาระบบการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องมาตรฐานสากลเพิ่มขึ้นร้อยละ ๙๐ ภายในปี ๒๕๗๐

ตัวชี้วัดที่ ๒ การแก้ไขเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีประสิทธิภาพ เพิ่มขึ้นร้อยละ ๙๐ ภายในปี ๒๕๗๐

ตัวชี้วัดที่ ๓ การจัดทำหรือพัฒนากลไก มาตรการ และแนวทางในการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์ รวมถึงการพัฒนาการสืบสวนสอบสวนอาชญากรรมทางไซเบอร์ เพิ่มขึ้น ร้อยละ ๖๐ ภายในปี ๒๕๗๐

ตัวชี้วัดที่ ๔ สถิติคดีเกี่ยวกับอาชญากรรมทางไซเบอร์ลดลงร้อยละ ๓๐ เมื่อเทียบกับปีก่อนหน้า

๔. กลยุทธ์

<u>กลยุทธ์หลักที่ ๑</u> การป้องกัน รับมือ และลดความเสี่ยงกับภัยคุกคามทางไซเบอร์ที่กระทบต่อระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กลยุทธ์ย่อยที่ ๑.๑ เสริมสร้างศักยภาพของกลไกและหน่วยงานระดับชาติ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (National Computer Emergency Response Team: NCERT) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectorial CERT) โดยมีการเชื่อมโยงการทำงานระหว่างกันอย่างเป็นระบบ เพื่อให้สามารถรักษาความมั่นคงปลอดภัยไซเบอร์ และแก้ไขเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

กลยุทธ์ย่อยที่ ๑.๒ ส่งเสริมให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมีมาตรฐานและแนวทางปฏิบัติในการป้องกัน รับมือ ลดความเสี่ยง รักษา และฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ที่เท่าทันต่อเหตุการณ์ที่สอดคล้องกับมาตรฐานสากล

กลยุทธ์ย่อยที่ ๑.๓ บูรณาการความร่วมมือภายในประเทศระหว่างหน่วยงานภาครัฐ ทั้งฝ่ายทหาร พลเรือน ตำรวจ ภาคเอกชน และภาคส่วนที่เกี่ยวข้อง ให้เป็นเครือข่ายความร่วมมือที่เข้มแข็ง เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมถึงสงครามไซเบอร์

กลยุทธ์ย่อยที่ ๑.๔ ส่งเสริมความร่วมมือระหว่างประเทศในการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในระดับทวิภาคีและพหุภาคี โดยแลกเปลี่ยนข้อมูลข่าวสาร ข่าวกรอง และความรู้ที่ทันต่อเหตุการณ์ และเสริมสร้างความสัมพันธ์ที่ดีในทุกระดับ เพื่อให้สามารถป้องกัน ลดความเสี่ยง รวมถึงรับมือกับภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้อย่างทันท่วงที

กลยุทธ์ย่อยที่ ๑.๕ ส่งเสริมให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานเอกชนที่เกี่ยวข้อง พร้อมทั้งพัฒนาทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่พนักงานเจ้าหน้าที่ เจ้าหน้าที่ หรือบุคลากรของทุกภาคส่วนที่เกี่ยวข้อง

กลยุทธ์ย่อยที่ ๑.๖ ส่งเสริมการเผยแพร่ความรู้เพื่อสร้างความตระหนักถึงความสำคัญของภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แก่องค์กรและบุคลากรภาครัฐ ภาคเอกชน และภาคประชาสังคมที่เกี่ยวข้อง

<u>กลยุทธ์หลักที่ ๒</u> การเสริมสร้างขีดความสามารถในการป้องกันและแก้ไขปัญหาการใช้ไซเบอร์เป็นช่องทางในการก่ออาชญากรรมทางไซเบอร์

กลยุทธ์ย่อยที่ ๒.๑ พัฒนากลไก มาตรการ และแนวทางที่เกี่ยวข้องกับการป้องกันและปราบปรามที่ครอบคลุมถึงการพัฒนาการเฝ้าระวังความเสี่ยงในการก่ออาชญากรรมทางไซเบอร์ การแจ้งเตือนเพื่อลดความเสี่ยงการก่ออาชญากรรมทางไซเบอร์ รวมถึงการติดตาม วิเคราะห์ และการประมวลผลข้อมูลตลอดจนพัฒนาการสืบสวนอาชญากรรมทางไซเบอร์ด้วยการนำเทคโนโลยีมาใช้ประโยชน์

กลยุทธ์ย่อยที่ ๒.๒ ส่งเสริมความร่วมมือหรือให้ความช่วยเหลือระหว่างหน่วยงานทั้งภายในประเทศและต่างประเทศ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากการก่ออาชญากรรมทางไซเบอร์ร่วมกัน

กลยุทธ์ย่อยที่ ๒.๓ เสริมสร้างความตระหนักรู้และพัฒนาขีดความสามารถแก่องค์กรและบุคลากรภาครัฐ ภาคเอกชน และภาคประชาสังคมที่เกี่ยวข้องให้มีความรู้ในการป้องกันตนเองจากอาชญากรรมทางไซเบอร์

๕. หน่วยงานเจ้าภาพรับผิดชอบบูรณาการขับเคลื่อน

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ