แนวทางการยกระดับ ดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี

NCSA สกมช

สารบัญ

หน้า

สารบัญรูปภาพ

หน้า

สารบัญตาราง

หน้า

บทสรุปผู้บริหาร

Global Cybersecurity Index : GCI หรือดัชนีด้านความมั่นคงปลอดภัยไซเบอร์โลกของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) เป็นตัวชี้วัดในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละประเทศ ซึ่งจะพิจารณาจากมาตรการ 5 ด้าน ได้แก่ ด้านกฎหมาย (Legal) ด้านเทคนิค (Technical) ด้านหน่วยงาน/นโยบาย (Organizational) ด้านการพัฒนาศักยภาพ (Capacity Development) และด้านความร่วมมือ (Cooperation) ซึ่งจากผลการจัดอันดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์โลก (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ประจำปี พ.ศ. 2563 โดยจัดอันดับจากการประเมินศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ในหมู่ประเทศสมาชิก ITU ปรากฏว่า ประเทศไทยได้รับการจัดอันดับที่ 44 จากทั้งหมด 194 ประเทศ ซึ่งในขณะเดียวกันประเทศเพื่อนบ้านได้มีการพัฒนาศักยภาพในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในทางที่ดีขึ้น ซึ่งผลการจัดอันดับดังกล่าวส่งผลสะท้อนต่อความเชื่อมั่นด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทย จึงมีความจำเป็นอย่างยิ่งที่ประเทศไทยจะต้องเร่งรัดการพัฒนาเพื่อยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์โลก (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ให้มีผลคะแนนและอันดับที่ดีขึ้น และเป็นที่ยอมรับในระดับสากล นำไปสู่การสร้างความเชื่อมั่นในการลงทุนทั้งจากภายในและต่างประเทศ ส่งผลให้ประชาชนมีความเป็นอยู่ที่ดีและมั่นคง

แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี ฉบับนี้ เป็นการดำเนินงานภายใต้โครงการจ้างที่ปรึกษาเพื่อจัดทำแผนปฏิบัติการสำหรับการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ซึ่งสอดคล้องกับนโยบายการบริหารราชการแผ่นดินของคณะรัฐมนตรีระยะสั้น (Short term) นโยบายหลักลำดับที่ 1.3 ประเด็นการขยายโอกาส นโยบายรองลำดับที่ 1.3.11 การป้องกันภัยพิบัติและภัยความมั่นคงรูปแบบใหม่ นโยบายย่อยลำดับที่ 1.3.11.2 การเพิ่มความปลอดภัยทางไซเบอร์ รวมถึงสอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565 – 2570 ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยสาระสำคัญของแนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี รายละเอียดดังนี้

วิสัยทัศน์

"ยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยให้มีศักยภาพตามมาตรฐานสากล"

พันธกิจ

1. พัฒนารากฐานสำคัญด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ
2. พัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในประเทศ
3. ยกระดับศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศให้เป็นไปตามมาตรฐานสากล
4. บูรณาการความร่วมมือทุกภาคส่วนเพื่อพัฒนาขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศ

เป้าหมาย

ประเทศไทยมีผลคะแนนการประเมินการจัดอันดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) **ไม่น้อยกว่า 95 คะแนน**

ยุทธศาสตร์ที่ 1 การเพิ่มขีดความสามารถและพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Enhancing Capabilities and Cybersecurity Proficiency)

กลยุทธ์ที่ 1 การส่งเสริมและสนับสนุนให้บุคลากรทุกระดับในประเทศมีความเข้าใจและตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ 2 การส่งเสริม สนับสนุน และพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในประเทศ

ยุทธศาสตร์ที่ 2 การบูรณาการความร่วมมือกับทุกภาคส่วนเพื่อรับมือภัยคุกคามทางไซเบอร์ (Integrating collaboration to confront cybersecurity threats)

กลยุทธ์ที่ 1 การบูรณาการความร่วมมือเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์

กลยุทธ์ที่ 2 การประสานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Empowering the Foundation of Cybersecurity)

กลยุทธ์ที่ 1 การขับเคลื่อนนโยบายและพัฒนากฎหมายให้ทันสมัยต่อภัยคุกคามทางไซเบอร์

กลยุทธ์ที่ 2 การผลักดันให้เกิดกลไกการคุ้มครองเด็กออนไลน์ (Child Online Protection) ที่สอดคล้องกับระดับสากล

กลยุทธ์ที่ 3 การยกระดับศักยภาพและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ที่ 4 การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)

กลยุทธ์ที่ 1 การส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ 2 การยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

แนวทางยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปีจัดทำขึ้นเพื่อเป็นกรอบแนวทางการยกระดับผลการประเมินดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ของประเทศไทย มีผลคะแนนการประเมินที่ดีขึ้น และนำไปสู่การปฏิบัติอย่างเป็นรูปธรรมต่อไป

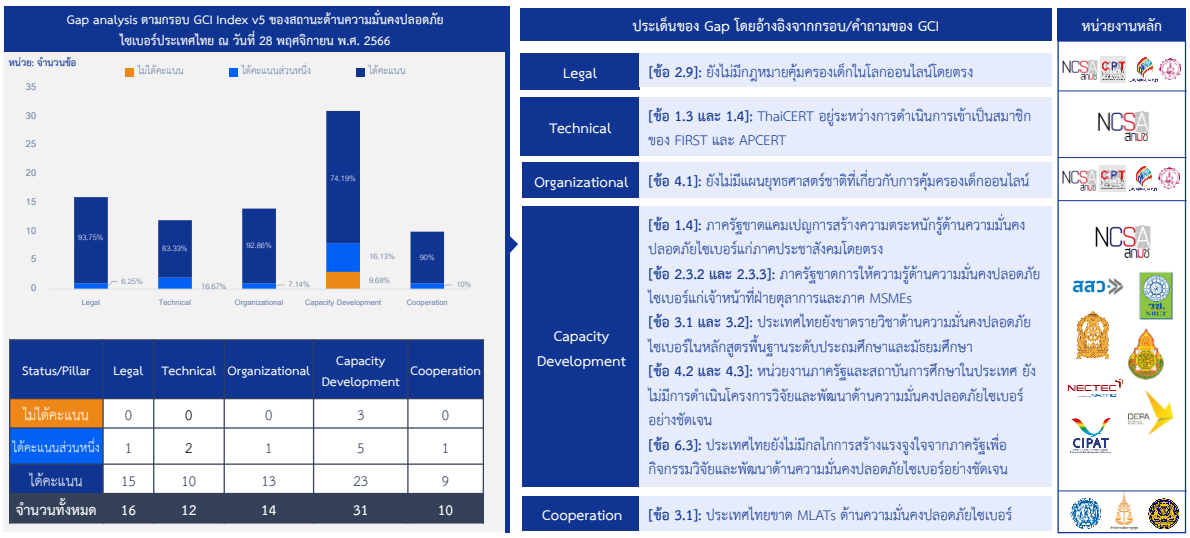
บทที่ 1
การจัดทำแนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทยระยะ 3 ปี

1.1 การวิเคราะห์สภาพแวดล้อมและศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย

การประเมินสภาพแวดล้อมและศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย พิจารณาจากการวิเคราะห์ช่องว่างการดำเนินงาน (Gap Analysis) โดยวิเคราะห์ตามประเด็นกรอบการประเมินดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) รวมถึงการวิเคราะห์ จุดแข็ง (S) จุดอ่อน (W) โอกาส (O) และอุปสรรค (T) ด้วยเครื่องมือ SWOT Analysis จากนั้นนำผลลัพธ์ที่ได้มาวิเคราะห์หาความสัมพันธ์ระหว่าง จุดแข็งและโอกาส (S-O) จุดแข็งและข้อจำกัด (S-T) จุดอ่อนและโอกาส (W-O) จุดอ่อนและข้อจำกัด (W-T) ด้วยการวิเคราะห์ TOWS Matrix เพื่อเป็นข้อมูลสนับสนุนในการจัด แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทยระยะ 3 ปี รายละเอียดดังนี้

1.1.1 การวิเคราะห์ช่องว่างการดำเนินงาน (Gap Analysis)

การวิเคราะห์ช่องว่างการดำเนินงาน (Gap Analysis) ของสถานภาพการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย เป็นการวิเคราะห์เพื่อหาช่องว่างการดำเนินงานในปัจจุบัน เทียบกับกรอบการประเมินดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) โดยพิจารณาว่ามีการดำเนินงานครบถ้วนตามกรอบการประเมินหรือไม่ เพื่อสามารถกำหนดแนวทางการดำเนินงานเพื่อปิดช่องว่างดังกล่าว ดังนี้



หมายเหตุ: Gap Analysis ข้างต้น อ้างอิงจากข้อมูลเมื่อวันที่ 28 พฤศจิกายน พ.ศ. 2566

รูปที่ 1 การวิเคราะห์ Gap Analysis ของสถานภาพด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ณ วันที่ 28 พฤศจิกายน พ.ศ. 2566

ด้านกฎหมาย (Legal Measure)

การประเมินด้านกฎหมาย (Legal Measure) ตามกรอบ/คำถามของดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับรอบปี พ.ศ. 2565 ประกอบไปด้วย 2 ตัวชี้วัดหลัก ได้แก่ กฎหมายอาชญากรรมไซเบอร์ (Cybercrime Law) และการกำกับดูแลความปลอดภัยทางไซเบอร์ (Cybersecurity Regulation) ภายใต้ประเด็นคำถามจำนวน 16 ข้อ

อ้างอิงจากข้อมูล ณ วันที่ 28 พฤศจิกายน พ.ศ. 2566 ประเทศไทยมีการดำเนินงานที่ครอบคลุมประเด็นคำถามจำนวน 15 ข้อ คิดเป็นสัดส่วนร้อยละ 93.75 และการดำเนินงานที่หลักฐานประกอบยังมีน้ำหนักไม่เพียงพอ จำนวน 1 ข้อ คิดเป็นสัดส่วนร้อยละ 6.25 ซึ่งอาจทำให้ได้รับการประเมินคะแนนเพียงบางส่วนในข้อ 2.9 ประเด็นการมีกฎระเบียบ/ข้อบังคับที่ครอบคลุมด้านการคุ้มครองเด็กออนไลน์ (Child Online Protection) โดยเฉพาะ

ด้านมาตรการทางเทคนิค (Technical Measure)

การประเมินด้านมาตรการทางเทคนิค (Technical Measure) ตามกรอบ/คำถามของดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับรอบปี พ.ศ. 2565 ประกอบไปด้วย 3 ตัวชี้วัดหลัก ได้แก่ การจัดตั้งหน่วยงาน National CERT/CIRT/CSIRT หรือ SOC การจัดตั้งหน่วยงาน Sectoral CERT/CIRT/CSIRT หรือ SOC และกรอบการดำเนินงานระดับชาติสำหรับการดำเนินการตามมาตรฐานความปลอดภัย ภายใต้ประเด็นคำถามจำนวน 12 ข้อ

อ้างอิงจากข้อมูล ณ วันที่ 28 พฤศจิกายน พ.ศ. 2566 ประเทศไทยมีการดำเนินงานที่ครอบคลุมประเด็นคำถามจำนวน 10 ข้อ คิดเป็นสัดส่วนร้อยละ 83.33 และการดำเนินงานที่หลักฐานประกอบยังมีน้ำหนักไม่เพียงพอ จำนวน 2 ข้อ คิดเป็นสัดส่วนร้อยละ 16.67 ในข้อ 1.3 และ 1.4 ประเด็นการเข้าร่วมเป็นสมาชิกของ Forum of Incident Response and Security Teams (FIRST) และสมาชิกของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในภูมิภาคเอเชียแปซิฟิก (Asia Pacific Computer Emergency Response Team: APCERT)

ด้านหน่วยงาน/นโยบาย (Organizational Measure)

การประเมินด้านหน่วยงาน/นโยบาย (Organizational Measure) ตามกรอบ/คำถามของดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับรอบปี พ.ศ. 2565 ประกอบไปด้วย 4 ตัวชี้วัดหลัก ได้แก่ ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cybersecurity Strategy) หน่วยงานที่รับผิดชอบ (Responsible agency) เมตริกความปลอดภัยทางไซเบอร์ (Cybersecurity metrics) กลยุทธ์และความคิดริเริ่มในการคุ้มครองเด็กออนไลน์ (Child Online Protection strategies and initiatives) ภายใต้ประเด็นคำถามจำนวน 14 ข้อ

อ้างอิงจากข้อมูล ณ วันที่ 28 พฤศจิกายน พ.ศ. 2566 ประเทศไทยมีการดำเนินงานที่ครอบคลุมประเด็นคำถามจำนวน 13 ข้อ คิดเป็นสัดส่วนร้อยละ 92.86 และการดำเนินงานที่หลักฐานประกอบยังมีน้ำหนักไม่เพียงพอ จำนวน 1 ข้อ คิดเป็นสัดส่วนร้อยละ 7.14 ซึ่งอาจทำให้ได้รับการประเมินคะแนนเพียงบางส่วนในข้อ 4.1 ประเด็นการมียุทธศาสตร์ระดับชาติเกี่ยวกับการคุ้มครองเด็กทางออนไลน์ โดยเกี่ยวข้องกับโครงการริเริ่มการคุ้มครองเด็กทางออนไลน์ในปัจจุบัน

ด้านการพัฒนาศักยภาพ (Capacity Development Measure)

การประเมินด้านการพัฒนาศักยภาพ (Capacity Development Measure) ตามกรอบ/คำถามของดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับรอบปี พ.ศ. 2565 ประกอบไปด้วย 6 ตัวชี้วัดหลัก ได้แก่ แคมเปญการรับรู้ความปลอดภัยทางไซเบอร์สาธารณะ (Public cybersecurity awareness campaigns) การฝึกอบรมสำหรับผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ (Training for cybersecurity professionals) โปรแกรมการศึกษาด้านความปลอดภัยทางไซเบอร์ซึ่งเป็นส่วนหนึ่งของหลักสูตรการศึกษาระดับชาติ (Cybersecurity educational programs as part of national academic curricula) โครงการวิจัยและพัฒนาความปลอดภัยทางไซเบอร์ (R&D) (Cybersecurity Research and Development (R&D) programs) อุตสาหกรรมความปลอดภัยทางไซเบอร์แห่งชาติ (National cybersecurity industry) และกลไกจูงใจภาครัฐ (Government incentive mechanisms) ภายใต้ประเด็นคำถามจำนวน 31 ข้อ

อ้างอิงจากข้อมูล ณ วันที่ 28 พฤศจิกายน พ.ศ. 2566 ประเทศไทยมีการดำเนินงานที่ครอบคลุมประเด็นคำถามจำนวน 23 ข้อ คิดเป็นสัดส่วนร้อยละ 74.19 และการดำเนินงานที่หลักฐานประกอบยังมีน้ำหนักไม่เพียงพอ จำนวน 8 ข้อ คิดเป็นสัดส่วนร้อยละ 25.81 ซึ่งอาจทำให้ได้รับการประเมินคะแนนเพียง

บางส่วนในข้อ 1.4 ประเด็นแคมเปญการรับรู้สาธารณะที่กำหนดเป้าหมายเฉพาะในภาคประชาสังคม ข้อ 2.3.2 ประเด็นการพัฒนาหรือสนับสนุนโปรแกรมการศึกษาด้านความปลอดภัยทางไซเบอร์หรือการฝึกอบรมสำหรับผู้ทำหน้าที่ตุลาการในระดับชาติ ข้อ 2.3.3 ประเด็นการพัฒนาหรือสนับสนุนโปรแกรมการศึกษาหรือการฝึกอบรมด้านความปลอดภัยในโลกไซเบอร์สำหรับ MSMEs ข้อ 3.1 และ 3.2 ประเด็นโปรแกรมการศึกษาด้านความปลอดภัยในโลกไซเบอร์ที่รวมอยู่ในหลักสูตรการศึกษาระดับประถมศึกษา และระดับมัธยมศึกษา ข้อ 4.2 และ 4.3 การดำเนินกิจกรรม R&D ที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์โดยสถาบันการศึกษา และข้อ 6.3 ประเด็นกลไกจูงใจของรัฐบาลในประเทศเพื่อส่งเสริมกิจกรรม R&D ที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

ด้านความร่วมมือ (Cooperation Measure)

การประเมินด้านความร่วมมือ (Cooperation Measure) ตามกรอบ/คำถามของดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับรอบปี พ.ศ. 2565 ประกอบไปด้วย 5 ตัวชี้วัดหลัก ได้แก่ ข้อตกลงความปลอดภัยทางไซเบอร์ระดับทวิภาคีกับประเทศอื่น ๆ (Bilateral cybersecurity agreement(s) with other countries) ข้อตกลงความปลอดภัยทางไซเบอร์แบบพหุภาคีกับประเทศอื่น ๆ (Multilateral cybersecurity agreements with other countries) สนธิสัญญาความช่วยเหลือทางกฎหมายร่วมกัน (MLAT) ที่เกี่ยวข้องกับความปลอดภัยในโลกไซเบอร์ (Mutual Legal Assistance Treaties (MLATs) related to cybersecurity) ความร่วมมือระหว่างภาครัฐและเอกชน (Public-Private Partnerships: PPPs) และความร่วมมือระหว่างหน่วยงาน (Inter-agency partnerships) ภายใต้ประเด็นคำถามจำนวน 10 ข้อ

อ้างอิงจากข้อมูล ณ วันที่ 28 พฤศจิกายน พ.ศ. 2566 ประเทศไทยมีการดำเนินงานที่ครอบคลุมประเด็นคำถามจำนวน 9 ข้อ คิดเป็นสัดส่วนร้อยละ 90 และการดำเนินงานที่หลักฐานประกอบยังมีน้ำหนักไม่เพียงพอ จำนวน 1 ข้อ คิดเป็นสัดส่วนร้อยละ 10 ซึ่งอาจทำให้ได้รับการประเมินคะแนนเพียงบางส่วนในข้อ 3.1 ประเด็นการเข้าร่วมในสนธิสัญญาความช่วยเหลือทางกฎหมายร่วมกัน (MLAT) เกี่ยวกับความปลอดภัยทางไซเบอร์ไม่ว่าจะผ่านข้อตกลงทวิภาคีหรือพหุภาคีกับประเทศอื่น ๆ หรือองค์กรระดับภูมิภาคหรือระหว่างรัฐบาลโดยเฉพาะ

1.1.2 การวิเคราะห์ SWOT Analysis

การการวิเคราะห์ จุดแข็ง (S) และ จุดอ่อน (W) เป็นการศึกษาวิเคราะห์ปัจจัยภายในของสถานภาพด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย และการวิเคราะห์ โอกาส (O) และอุปสรรค (T) เป็นการศึกษาวิเคราะห์ปัจจัยภายนอกของสถานภาพด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย ซึ่งจะสามารถกำหนดแนวทางในการวางกลยุทธ์ของ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี ที่ชัดเจน

จุดแข็ง (Strengths: S)
S1 มีความพร้อมด้านกฎหมายและกฎหมายลำดับรองที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์
S2 มีหน่วยงานกลางที่รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ
S3 มีหน่วยงานภายใต้การกำกับดูแลที่จัดการด้านความมั่นคงปลอดภัยไซเบอร์ในแต่ละภาคส่วน (CII Agencies)

จุดอ่อน (Weaknesses: W)
W1 ขาดแคลนบุคลากรที่มีทักษะด้านความมั่นคงปลอดภัยไซเบอร์ระดับสูง
W2 ขาดการบูรณาการการทำงานระหว่างหน่วยงานภาครัฐและการร่วมมือกับภาคเอกชน
W3 ขาดการส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์จากภาครัฐ
W4 ขาดการเข้าร่วมกับองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศ
W5 ข้อจำกัดในการจัดหาและจัดสรรงบประมาณ
W6 หน่วยงานในประเทศไทยยังไม่ได้เป็น Partner ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU)

โอกาส (Opportunities: O)
O1 การเติบโตของอุตสาหกรรมไซเบอร์ทั่วโลกทำให้มีโอกาสเกิดแรงงานด้านไซเบอร์มากขึ้น
O2 การพัฒนาอย่างต่อเนื่องของเทคโนโลยีทำให้ประสิทธิภาพในการรักษาความมั่นคงปลอดภัย

ไซเบอร์สูงขึ้น O3 ประชาชนมีความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้น เนื่องจากภัยคุกคามทางไซเบอร์ในปัจจุบัน

อุปสรรค (Threats: T)
T1 การเติบโตของภัยคุกคามทางไซเบอร์จากทั่วโลกทั้งในเชิงรูปแบบและปริมาณ T2 ภาวะเศรษฐกิจถดถอย ทำให้งบประมาณของทุกประเทศทั่วโลกลดลง T3 เหตุการณ์ความไม่สงบจากทั่วโลก ทำให้มีโอกาสเกิดการจารกรรมหรือสอดแนมทางไซเบอร์ (Cyber Espionage) T4 การแข่งขันในด้านความมั่นคงปลอดภัยไซเบอร์จากทั่วโลกสูงขึ้น

1.1.3 การวิเคราะห์ TOWS Matrix

หลังจากจากการวิเคราะห์ จุดแข็ง (S) และ จุดอ่อน (W) โอกาส (O) และอุปสรรค (T) ของสถานภาพด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทย โดยการวิเคราะห์ SWOT Analysis แล้วสามารถนำผลลัพธ์ที่ได้มากำหนดกลยุทธ์ของ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี ด้วยการใช้หลักการ TOWS Matrix ซึ่งเป็นเครื่องมือที่นิยมนำมาใช้ในการกำหนดกลยุทธ์ โดยผลลัพธ์จากการวิเคราะห์จะประกอบด้วยกลยุทธ์ในการพัฒนา 4 รูปแบบ ได้แก่ กลยุทธ์เชิงรุก กลยุทธ์เชิงป้องกัน กลยุทธ์เชิงแก้ไข และกลยุทธ์เชิงรับ รายละเอียดดังนี้

ปัจจัยภายใน / ปัจจัยภายนอก	จุดแข็ง (S)	จุดอ่อน (W)
	S1 มีความพร้อมด้านกฎหมายและกฎหมายลำดับรองที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ S2 มีหน่วยงานกลางที่รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ S3 มีหน่วยงานภายใต้การกำกับดูแลที่จัดการด้านความมั่นคงปลอดภัยไซเบอร์ในแต่ละภาคส่วน (CII Agencies)	W1 ขาดแคลนบุคลากรที่มีทักษะด้านความมั่นคงปลอดภัยไซเบอร์ระดับสูง W2 ขาดการบูรณาการการทำงานระหว่างหน่วยงานภาครัฐและการร่วมมือกับภาคเอกชน W3 ขาดการส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์จากภาครัฐ W4 ขาดการเข้าร่วมกับองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศ W5 ข้อจำกัดในการจัดหาและจัดสรรงบประมาณ W6 หน่วยงานในประเทศไทยยังไม่ได้เป็น Partner ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU)
โอกาส (O)	**กลยุทธ์เชิงรุก (S/O)**	**กลยุทธ์เชิงแก้ไข (W/O)**
O1 การเติบโตของอุตสาหกรรมไซเบอร์ทั่วโลกทำให้มีโอกาสเกิดแรงงานด้านไซเบอร์มากขึ้น	• การยกระดับศักยภาพและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์	

O2 การพัฒนาอย่างต่อเนื่องของเทคโนโลยีทำให้ประสิทธิภาพในการรักษาความมั่นคงปลอดภัยไซเบอร์สูงขึ้น O3 ประชาชนมีความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพิ่มขึ้น เนื่องจากภัยคุกคามทางไซเบอร์ในปัจจุบัน	• การผลักดันให้เกิดกลไกการคุ้มครองเด็กออนไลน์ (Child Online Protection) ที่สอดคล้องกับระดับสากล • ส่งเสริมและสนับสนุนให้บุคลากรทุกระดับในประเทศมีความเข้าใจและตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์	• การส่งเสริม สนับสนุน และพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในประเทศ • การส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์
อุปสรรค (T) T1 การเติบโตของภัยคุกคามทางไซเบอร์จากทั่วโลกทั้งในเชิงรูปแบบและปริมาณ T2 ภาวะเศรษฐกิจถดถอย ทำให้งบประมาณของทุกประเทศทั่วโลกลดลง T3 เหตุการณ์ความไม่สงบจากทั่วโลก ทำให้มีโอกาสเกิดการจารกรรมหรือสอดแนมทางไซเบอร์ (Cyber Espionage) T4 การแข่งขันในด้านความมั่นคงปลอดภัยไซเบอร์จากทั่วโลกสูงขึ้น	**กลยุทธ์เชิงป้องกัน (S/T)** • การขับเคลื่อนนโยบายและพัฒนากฎหมายให้ทันสมัยต่อภัยคุกคามทางไซเบอร์ • การยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์	**กลยุทธ์เชิงรับ (W/T)** • การประสานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์ • การบูรณาการความร่วมมือเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์

ตารางที่ 10 ผลการวิเคราะห์ TOWS Matrix

1.2 วิสัยทัศน์ พันธกิจ และเป้าหมาย

1.2.1 วิสัยทัศน์

“ยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยให้มีศักยภาพตามมาตรฐานสากล”

1.2.2 พันธกิจ

พันธกิจของ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทยระยะ 3 ปี ประกอบไปด้วย 4 พันธกิจ ดังนี้

1. พัฒนารากฐานสำคัญด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

2. พัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในประเทศ

3. ยกระดับศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศให้เป็นไปตามมาตรฐานสากล

4. บูรณาการความร่วมมือทุกภาคส่วนเพื่อพัฒนาขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศ

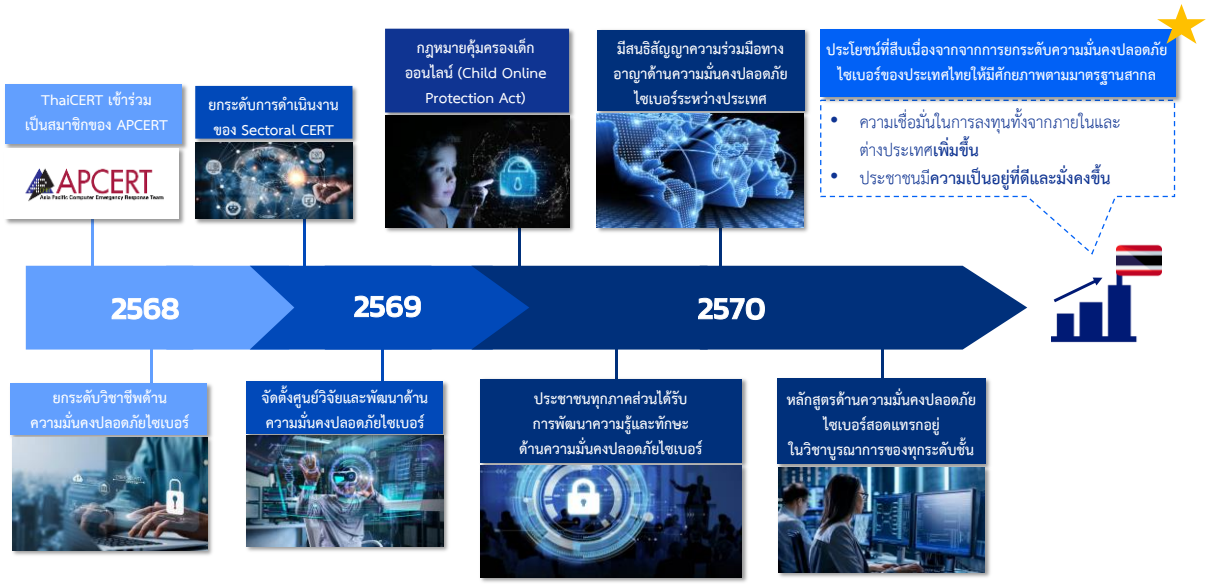
1.2.3 เป้าหมาย

ประเทศไทยมีผลคะแนนการประเมินการจัดอันดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) **ไม่น้อยกว่า 95 คะแนน**

1.3 ภูมิทัศน์ปลายทางของ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย

ภายในระยะเวลา 3 ปี (พ.ศ. 2568 – พ.ศ. 2570) ประเทศไทยมีการยกระดับผลการประเมินดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ให้มีศักยภาพตามมาตรฐานสากล โดยมีผลคะแนนการประเมินไม่น้อยกว่า 95 คะแนน จากเดิม 86.5 คะแนน ในปี พ.ศ. 2563 การประเมินดัชนีความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) เป็นการประเมินศักยภาพและความพร้อมในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศที่เป็นสมาชิก การประเมินพิจารณาจากปัจจัย 5 ด้าน ได้แก่ ด้านกฎหมาย (Legal Measure) ด้านมาตรการทางเทคนิค (Technical Measure) ด้านหน่วยงาน/นโยบาย (Organizational Measure) ด้านการพัฒนาศักยภาพ (Capacity Development Measure) และด้านความร่วมมือ (Cooperation Measure) การพัฒนาทั้ง 5 ด้านนี้ ส่งผลให้ประเทศไทยเกิดการยกระดับดัชนีความมั่นคงปลอดภัยไซเบอร์และเป็นที่ยอมรับจากสากล ผ่านการพัฒนาภายใต้พันธกิจ 4 ประเด็น ดังนี้

1. พัฒนารากฐานสำคัญด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ
2. พัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในประเทศ
3. ยกระดับศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศให้เป็นไปตามมาตรฐานสากล
4. บูรณาการความร่วมมือทุกภาคส่วนเพื่อพัฒนาขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศ



รูปที่ 2 ภูมิทัศน์ปลายทางของ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย

ภายในปี พ.ศ. 2570 ประเทศไทยได้ดำเนินการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ตามแผนภายใต้ยุทธศาสตร์ทั้ง 4 ข้อ ผ่านกลไกการเพิ่มขีดความสามารถและพัฒนาศักยภาพของบุคลากร การบูรณาการและการวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ รวมไปถึงการยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้เพื่อให้สอดคล้องกับวิสัยทัศน์ "ยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยให้มีศักยภาพตามมาตรฐานสากล" ตามที่กำหนดไว้ในแผนปฏิบัติการ สามารถสะท้อนออกมาเป็นภาพรวมของภูมิทัศน์การพัฒนา ดังนี้

ปี พ.ศ. 2568 ประเทศไทยมีการกำหนดเป้าหมายสำหรับการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ในด้านมาตรการทางเทคนิค โดยมีการยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) เพื่อให้มีการดำเนินงานตามมาตรฐานสากล ไม่ว่าจะเป็นการเพิ่มประสิทธิภาพเครื่องมือทางเทคนิคที่จำเป็นในการดำเนินงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ การพัฒนาระบบเฝ้าระวัง ตรวจจับ รับมือ แก้ปัญหา รวมไปถึงทักษะของบุคลากร เป็นต้น ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) เข้าร่วมเป็นสมาชิกของ APCERT (Asia Pacific Computer Emergency Response Team) โดยมุ่งเน้นให้เกิดการประสานงานกันอย่างมีประสิทธิภาพ เพื่อเสริมสร้างความแข็งแกร่งในด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ซึ่งเป็นสิ่งสำคัญเพื่อเสริมสร้างความร่วมมือในการรับมือกับปัญหาความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศ ส่งผลต่อความเชื่อมั่นด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย รวมไปถึงความเชื่อมั่นในการลงทุนทั้งจากภายในและต่างประเทศ นอกจากนี้ในด้านหน่วยงาน/นโยบายยังมีการจัดทำกรอบแนวคิด เครื่องมือหรือตัวแบบในการประเมินระดับศักยภาพและความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อกรอบการประเมินศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Self-Assessment) ประเทศไทยได้ทำการศึกษาแนวคิดและเครื่องมือที่มีมาตรฐานสากล ซึ่งจะช่วยให้กระบวนการประเมินมีความเที่ยงตรง และมีประสิทธิภาพมากยิ่งขึ้น เพื่อสนับสนุนการพัฒนาและปรับปรุงทักษะในด้านความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ประเทศไทยยังมีการส่งเสริมและสนับสนุนการรับรองหลักสูตรวิชาชีพทางความมั่นคงปลอดภัยไซเบอร์ และเตรียมพร้อมในการทำงานในสาขาอาชีพที่เกี่ยวข้อง ทั้งนี้ การดำเนินงานและการพัฒนาทางด้านความมั่นคงปลอดภัยไซเบอร์นี้ ส่งผลให้ประเทศไทยมีรากฐานที่แข็งแกร่งในการรับมือกับภัยคุกคามทางไซเบอร์ และสร้างสภาพแวดล้อมที่ปลอดภัยและมั่นคงของประชาชนในประเทศ

ปี พ.ศ. 2569 ประเทศไทยมีการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ในด้านการพัฒนาศักยภาพ มีการวิจัยและพัฒนานวัตกรรมและเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ ภายใต้การดำเนินงานของสถาบันการศึกษาในประเทศ เนื่องจากการโจมตีทางไซเบอร์มีความหลากหลายและมีความท้าทายอย่างต่อเนื่อง การศึกษาพัฒนาและรักษาความมั่นคงปลอดภัยในด้านนี้จึงเป็นสิ่งจำเป็น นอกจากนี้เพื่อส่งเสริมให้เกิดการวิจัยและพัฒนานวัตกรรมและเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ มีการสนับสนุนทุนการศึกษาอย่างต่อเนื่อง สำหรับบุคลากรทั่วไป หน่วยงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ นักศึกษา และนักวิจัย ทั้งนี้ ในด้านมาตรการทางเทคนิค ประเทศไทยมีการยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) ให้มีการดำเนินงานตามมาตรฐานสากล โดยมีการดำเนินภารกิจการประสานงาน การเฝ้าระวังการรับมือภัยคุกคามทางไซเบอร์ และมาตรการด้านการบริหารจัดการคุณภาพ ผ่านระบบพี่เลี้ยง (Mentoring) ตามพระราชบัญญัติ ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยสมบูรณ์ครบถ้วน ส่งผลให้สามารถตรวจจับและรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ

ปี พ.ศ. 2570 ประเทศไทยมุ่งมั่นในการยกระดับด้านความมั่นคงปลอดภัยไซเบอร์ผ่านการเล็งเห็นเป้าหมายในด้านต่าง ๆ ของแผนปฏิบัติการ โดยมีแผนการดำเนินการที่หลากหลายและครอบคลุมทุกระดับชั้นของประชาชน เพื่อให้ประชาชนทุกภาคส่วนมีความรู้ และทักษะที่เพียงพอในการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งนี้ คาดว่าจะส่งผลให้มีการวิจัยและพัฒนานวัตกรรมและเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์เกิดขึ้นในปีนี้ พร้อมทั้งการพัฒนาความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ให้กับประชาชนทุกภาคส่วน โดยการฝึกอบรมผ่านโปรแกรมการศึกษาที่ถูกพัฒนาขึ้นผ่านแพลตฟอร์ม E-Learning หรือสื่อออนไลน์อื่น ๆ เพื่อให้ประชาชนทุกภาคส่วนสามารถเข้าถึงได้ง่าย และได้รับประสบการณ์การการเรียนรู้ที่ยืดหยุ่นและตรงกับความต้องการของกลุ่มเป้าหมาย รวมทั้งพัฒนาหลักสูตรการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดแทรกอยู่ในวิชาบูรณาการของทุกระดับชั้น เพื่อให้เกิดความตระหนักรู้ ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ตั้งแต่วัยเรียน นอกจากนี้ยังมีการเสริมสร้างความร่วมมือระหว่างประเทศที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ โดยการเข้าร่วมโครงการและกิจกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคอาเซียน และระดับนานาชาติ อีกทั้งยังได้ตรวจสอบและเพิ่มเติมกฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ รวมถึงการคุ้มครองเด็กออนไลน์ การดำเนินการนี้ส่งผลให้เกิดการปกป้องคุ้มครองเด็กและเยาวชนจากการละเมิดทางออนไลน์ เช่น การล่อลวง การแสวงหาประโยชน์ทางเพศ และการสะกดรอยทางออนไลน์ ซึ่งทำให้มีโอกาสเกิดสนธิสัญญาความร่วมมือทางอาญาด้านความมั่นคงปลอดภัยไซเบอร์ระหว่าง

ประเทศได้มากขึ้น การยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยในครั้งนี้ ส่งผลให้ประเทศไทยสามารถเรียกความเชื่อมั่นทางด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และความเชื่อมั่นในการลงทุนจากทั้งภายในประเทศ และต่างประเทศ เป็นการสร้างสภาพแวดล้อมทางธุรกิจที่มั่งคงและเป็นประโยชน์ และส่งผลให้ประชาชนให้มีความเป็นอยู่ที่ดีและมั่งคงขึ้นในยุคที่เทคโนโลยีมีบทบาทสำคัญในทุก ๆ ด้านของชีวิตประจำวัน

1.4 ความเชื่อมโยงของแผน

แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี สอดคล้องกับนโยบายการบริหารราชการแผ่นดินของคณะรัฐมนตรีระยะสั้น (Short term) นโยบายหลักลำดับที่ 1.3 ประเด็นการขยายโอกาส นโยบายรองลำดับที่ 1.3.11 การป้องกันภัยพิบัติและภัยความมั่นคงรูปแบบใหม่ นโยบายย่อยลำดับที่ 1.3.11.2 เพิ่มความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงมีการดำเนินงานที่สอดคล้องตามนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

รูปที่ 1 ความเชื่อมโยงของแผนปฏิบัติการ

สาระสำคัญของ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี ตามประเด็นยุทธศาสตร์และกลยุทธ์ของนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570) ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีดังนี้

ยุทธศาสตร์ที่ 1 สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Capacity)

กลยุทธ์ที่ 1.1 เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ 1.2 สร้างความตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ 1.3 ส่งเสริมการวิจัยและพัฒนาและนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)

กลยุทธ์ที่ 2.1 ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและภาคเอกชน

กลยุทธ์ที่ 2.2 ประสานความร่วมมือระหว่างประเทศเพื่อรับมือภัยคุกคาม

ยุทธศาสตร์ที่ 3 สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Resilience)

กลยุทธ์ที่ 3.1 กำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII)

กลยุทธ์ที่ 3.2 กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กลยุทธ์ที่ 3.3 ปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ

ยุทธศาสตร์ที่ 4 สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน (Standard)

กลยุทธ์ที่ 4.1 เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ 4.2 ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม

กลยุทธ์ที่ 4.3 ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์

1.5 ยุทธศาสตร์และกลยุทธ์

แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี ประกอบไปด้วย 4 ยุทธศาสตร์ ดังนี้

รูปที่ 3 ยุทธศาสตร์และกลยุทธ์ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี

1.5.1 ยุทธศาสตร์ที่ 1 การเพิ่มขีดความสามารถและพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ (Enhancing Capabilities and Cybersecurity Proficiency)

เป้าหมายยุทธศาสตร์

1. บุคลากรทุกระดับในประเทศ มีทักษะ ความรู้ ความสามารถ และความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์
2. ส่งเสริมและพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์เพื่อรองรับความต้องการของประเทศ

ตัวชี้วัดยุทธศาสตร์

1. กลุ่มเป้าหมายที่เกี่ยวข้องกับโครงการได้รับการพัฒนาความรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ไม่น้อยกว่าร้อยละ 80

2. มีหลักสูตรการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์หรือที่เกี่ยวข้อง ในระดับประถมศึกษา ระดับมัธยมศึกษา และระดับอุดมศึกษา

3. มีการรับรองหลักสูตรวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์

4. มีการออกใบรับรอง (Certification) ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

กลยุทธ์ที่ 1 การส่งเสริมและสนับสนุนให้บุคลากรทุกระดับในประเทศมีความเข้าใจและตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
1	โครงการผลักดันความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาศักยภาพบุคลากรระดับชาติ	✓	✓	✓	270,000,000	**หลัก**: สกมช. (สวม.) **รอง**: สพร./ สพธอ./ สดช./ สอศ./ สพฐ./ อว./ ดศ./ ตร./ สสว./ ปค./ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
2	โครงการเสริมสร้างความเข้าใจและตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติ	✓	✓	✓	24,000,000	**หลัก**: สกมช. (สวม.) **รอง**: สพร./ สพธอ./ สดช./ สอศ./ สพฐ./ อว./ ดศ./ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
3	โครงการฝึกซ้อมแนวทางปฏิบัติเพื่อรับมือภัยคุกคามทางไซเบอร์ในระดับวิกฤตในประเทศ	✓	✓	✓	84,000,000	**หลัก**: สกมช. (สบพ.) **รอง**: หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ตารางที่ 1 โครงการภายใต้ ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 1

กลยุทธ์ที่ 2 การส่งเสริม สนับสนุน และพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในประเทศ

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
1	โครงการผลักดัน ส่งเสริม และสนับสนุนการพัฒนาหลักสูตรการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์	✓	✓	✓	18,000,000	**หลัก**: สกมช. (ศวจ.) **รอง**: สำนักงาน ก.พ./ สคช./ สดช./ สอศ./ สพฐ./ ศธ./ สช./ อว./ ดศ./ บก./ ทท./ สปท. สำนักงบประมาณ/ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
2	โครงการส่งเสริมและสนับสนุนการรับรองหลักสูตรวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์	✓	-	-	10,000,000	**หลัก**: สกมช. / กพร./ สคช. **รอง**: สพร./ สพธอ./ สำนักงาน ก.พ./ อว./ สดช./ สอศ./ สพฐ./ ดศ./ ส.ท.อ./ สำนักงบประมาณ
3	โครงการส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) แก่ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์	✓	✓	-	10,000,000	**หลัก:** สกมช. (ศวจ.)/ สคช. **รอง**: สพร./ สพธอ./ สำนักงาน ก.พ./ ดศ./ สคช./ สอศ./ อว./ บก./ ทท./ สปท./ บีโอไอ/ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ตารางที่ 2 โครงการภายใต้ ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 2

1.5.2 ยุทธศาสตร์ที่ 2 การบูรณาการความร่วมมือกับทุกภาคส่วนเพื่อรับมือภัยคุกคามทางไซเบอร์ (Integrating collaboration to confront cybersecurity threats)

เป้าหมายยุทธศาสตร์

1. ประเทศไทยมีการบูรณาการความร่วมมือกับทุกภาคส่วนทั้งในและต่างประเทศเพื่อยกระดับขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ของประเทศ

2. ประเทศไทยมีการผลักดันให้เกิดสนธิสัญญาความร่วมมือทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดยุทธศาสตร์

1. มีความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศในทุกมิติ ได้แก่ การบังคับใช้กฎหมาย การแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ และการพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์

2. มีกิจกรรมส่งเสริมและสนับสนุนความร่วมมือระหว่างหน่วยงานภาครัฐ เพื่อเสริมสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ

3. มีกิจกรรมส่งเสริมและสนับสนุนความร่วมมือระหว่างหน่วยงานเอกชน เพื่อยกระดับขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์ของประเทศ

4. มีสนธิสัญญาความร่วมมือทางอาญาระหว่างประเทศ (Mutual Legal Assistance Treaty – MLATs) ด้านความมั่นคงปลอดภัยไซเบอร์โดยเฉพาะ

กลยุทธ์ที่ 1 การบูรณาการความร่วมมือเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
1	โครงการบูรณาการความร่วมมือระหว่างประเทศเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย	✓	✓	✓	45,000,000	**หลัก:** สกมช. (สปส.) **รอง:** สพร./ สพธอ./ กต./ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
2	โครงการบูรณาการความร่วมมือระหว่างหน่วยงานภาครัฐเพื่อเสริมสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ	✓	✓	✓	90,000,000	**หลัก:** สกมช. (ศวจ.) **รอง:** สพร./ สพธอ./ ตร./ สำนักอัยการสูงสุด (อส.)/ หน่วยงานควบคุมหรือกำกับดูแล/ ยธ./ กห./ บก./ ทท.
3	โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย	✓	✓	✓	135,000,000	**หลัก:** สกมช. (สปส./ศวจ.) **รอง:** สพร./ สพธอ./ ตร./ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ตารางที่ 3 โครงการภายใต้ ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 1

กลยุทธ์ที่ 2 การประสานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
1	โครงการจัดประชุมภาคีเครือข่ายเพื่อส่งเสริมการพัฒนาความร่วมมือทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์	✓	✓	✓	15,000,000	**หลัก:** สกมช. (สกม.) **รอง:** สำนักอัยการสูงสุด (อส.)/ กต./ สคก.

ตารางที่ 4 โครงการภายใต้ ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 2

1.5.3 ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Empowering the Foundation of Cybersecurity)

เป้าหมายยุทธศาสตร์

1. ประเทศไทยมีกฎหมายและระเบียบด้านความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุม ทันสมัย และสอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต

2. ประเทศไทยมีการยกระดับศักยภาพและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องในระดับสากล

ตัวชี้วัดยุทธศาสตร์

1. มีกฎหมาย กฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมตามกรอบการประเมินดัชนีชี้วัดด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU)

2. มีกฎหมาย กฎระเบียบ ข้อบังคับ และแนวทางการคุ้มครองเด็กออนไลน์ (Child Online Protection) ที่เป็นไปตามมาตรฐานสากล

3. มีมาตรฐานการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ

4. มีมาตรฐานความมั่นคงปลอดภัยไซเบอร์สำหรับผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร

5. มีกรอบการประเมินความพร้อมและศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐและเอกชน

กลยุทธ์ที่ 1 การขับเคลื่อนนโยบายและพัฒนากฎหมายให้ทันสมัยต่อภัยคุกคามทางไซเบอร์

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
1	โครงการผลักดันการทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านอาชญากรรมไซเบอร์	✓	✓	✓	15,000,000	**หลัก:** สกมช. (สปบ.) / ดศ. **รอง:** ยธ./ สพร./ สพธอ./ สคส./

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
						หน่วยงานควบคุมหรือกำกับดูแล
2	โครงการทบทวน ปรับปรุง และพัฒนากฎหมายและระเบียบที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์	✓	-	✓	30,000,000	**หลัก:** สกมช. (สกม.) **รอง:** สคส./ ยธ./ กห./ ตร./ สพร./ สพธอ./ หน่วยงานควบคุมหรือกำกับดูแล/
3	โครงการติดตาม ทบทวน และปรับปรุงนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ประจำปี	✓	✓	✓	12,000,000	**หลัก:** สกมช. (สยศ.) **รอง:** หน่วยงานของรัฐ/ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ตารางที่ 5 โครงการภายใต้ ยุทธศาสตร์ที่ 3 กลยุทธ์ที่ 1

กลยุทธ์ที่ 2 การผลักดันให้เกิดกลไกการคุ้มครองเด็กออนไลน์ (Child Online Protection) ที่สอดคล้องกับระดับสากล

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
1	โครงการผลักดัน พัฒนากฎหมายคุ้มครองเด็กออนไลน์ (Child Online Protection Act)	✓	✓	✓	1,500,000	**หลัก:** สกมช. (สกม.)/ ดย.

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
						รอง: พม./ สคก./ ยธ./ ดศ./ ศธ./ มูลนิธิอินเทอร์เน็ตร่วมพัฒนาไทย
2	โครงการความร่วมมือเพื่อทบทวน พัฒนาและปรับปรุง แผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. 2566 - 2570	✓	✓	✓	1,500,000	**หลัก:** สกมช. (สยศ. และ สกม.)/ ดย. **รอง:** พม./ สคก./ ยธ./ ดศ./ ศธ./ มูลนิธิอินเทอร์เน็ตร่วมพัฒนาไทย

ตารางที่ 6 โครงการภายใต้ ยุทธศาสตร์ที่ 3 กลยุทธ์ที่ 2

กลยุทธ์ที่ 3 การยกระดับศักยภาพและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
1	โครงการพัฒนากรอบการดำเนินงานระดับชาติด้านมาตรฐานความมั่นคงปลอดภัยไซเบอร์	✓	-	✓	10,000,000	**หลัก:** สกมช. (สบพ.) **รอง:** สพร./ สพธอ./ หน่วยงานควบคุมหรือกำกับดูแล
2	โครงการจัดทำกรอบการประเมินศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ของ	✓	✓	✓	22,500,000	**หลัก:** สกมช. (สบพ.) **รอง:** หน่วยงานของรัฐ/ หน่วยงาน

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
	ประเทศ (Cybersecurity Self-Assessment)					ควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
3	โครงการส่งเสริมการประเมินและให้การรับรองมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ของผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร	-	-	✓	3,000,000	**หลัก:** สกมช. (ศวจ.)/ DEPA **รอง:** สมอ./ส.อ.ท./ สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์/ สมาคมความมั่นคงปลอดภัยสารสนเทศ

ตารางที่ 7 โครงการภายใต้ ยุทธศาสตร์ที่ 3 กลยุทธ์ที่ 3

1.5.4 ยุทธศาสตร์ที่ 4 การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)

เป้าหมายยุทธศาสตร์

1. ประเทศไทยมีการส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์
2. ประเทศไทยมีการยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) ให้มีการดำเนินงานตามมาตรฐานสากล

ตัวชี้วัดยุทธศาสตร์

1. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT) เข้าร่วมเป็นสมาชิกของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในระดับภูมิภาค และ The Forum of Incident Response and Security Teams หรือ FIRST
2. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) มีการดำเนินงานที่ครอบคลุมตามกรอบการประเมินดัชนีชี้วัดด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ไม่น้อยกว่าร้อยละ 80
3. มีสถาบันหรือศูนย์วิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ
4. มีมาตรการจูงใจเพื่อสนับสนุนการวิจัยและพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ

กลยุทธ์ที่ 1 การส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
1	โครงการส่งเสริมและสนับสนุนทุนการวิจัยและพัฒนา นวัตกรรม และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์	✓	✓	✓	45,000,000	**หลัก:** สกมช. (ศวจ.) **รอง:** หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐาน

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
						สำคัญทางสารสนเทศ/ สพร./ สพธอ./ สำนักงาน ก.พ./ สดช./ สอศ./ สพฐ./ อว./วช./ สวทช./ สทป./ บก./ ทท./ บีโอไอ / NIA
2	โครงการประสานความร่วมมือกับสถาบันการศึกษาเพื่อวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์	✓	✓	-	10,000,000	**หลัก:** สกมช. (ศวจ.) สวทช./ NECTEC **รอง:** ศธ./ อว./ วช./ สถาบันการศึกษาที่เกี่ยวข้อง เช่น MU KMITL KMUTT SPU
3	โครงการส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชันและผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ	✓	✓	✓	6,000,000	**หลัก:** สกมช. (ศวจ.) **รอง:** หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ/ สพร./ สพธอ./ สำนักงาน ก.พ./ สคช./ สดช./ สอศ./ สพฐ./ อว./ ดศ./ สทป./ บก./ ทท./ บีโอไอ /

ลำดับ	โครงการ	ปี 68	ปี 69	ปี 70	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
						ธปท./ ส.อ.ท./ สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์

ตารางที่ 8 โครงการภายใต้ ยุทธศาสตร์ที่ 4 กลยุทธ์ที่ 1

กลยุทธ์ที่ 2 การยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

ลำดับ	โครงการ	ปี 67	ปี 68	ปี 69	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
1	โครงการยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT)	✓	✓	✓	43,000,000	**หลัก:** สกมช. (สปบ.) / ThaiCERT
2	โครงการยกระดับการดำเนินการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)	✓	✓	✓	30,000,000	**หลัก:** สกมช. (สปส.) **รอง:** หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
3	โครงการสนับสนุนการเผยแพร่และประชาสัมพันธ์กิจกรรมการดำเนินงานของหน่วยงานควบคุมหรือกำกับดูแลและศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)	✓	-	-	40,000,000	**หลัก:** สกมช. (สปส.)/ ศูนย์ประสานความมั่นคงปลอดภัยระบบสารสนเทศ (Sectoral CERT) **รอง:** หน่วยงานควบคุมหรือกำกับดูแล

ลำดับ	โครงการ	ปี 67	ปี 68	ปี 69	งบประมาณ (บาท)	หน่วยงานที่รับผิดชอบ
4	โครงการพัฒนาแพลตฟอร์มสำหรับการแลกเปลี่ยนเหตุการณ์ภัยคุกคามทางไซเบอร์	✓	✓	✓	60,000,000	**หลัก:** สกมช. (สปส.)

ตารางที่ 9 โครงการภายใต้ ยุทธศาสตร์ที่ 4 กลยุทธ์ที่ 2

บทที่ 2

รายละเอียดขอบเขตการดำเนินงานของโครงการภายใต้ แนวทางการยกระดับฯ

รายละเอียดขอบเขตการดำเนินงานของโครงการ ภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทยระยะ 3 ปี มีรายละเอียดดังนี้

ยุทธศาสตร์	กลยุทธ์	งบประมาณ (ล้านบาท)			
		2568	2569	2570	รวม
ยุทธศาสตร์ที่ 1: การเพิ่มขีดความสามารถและพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Enhancing Capabilities and Cybersecurity Proficiency)	**กลยุทธ์ที่ 1:** การส่งเสริมและสนับสนุนให้บุคลากรทุกระดับในประเทศมีความเข้าใจและตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์	158	110	110	**378**
	กลยุทธ์ที่ 2: การส่งเสริม สนับสนุน และพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในประเทศ	21	11	6	**38**
ยุทธศาสตร์ที่ 2: การบูรณาการความร่วมมือกับทุกภาคส่วนเพื่อรับมือภัยคุกคามทางไซเบอร์ (Integrating collaboration to confront cybersecurity threats)	**กลยุทธ์ที่ 1:** การบูรณาการความร่วมมือเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์	45	45	45	**135**
	กลยุทธ์ที่ 2: การประสานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์	5	5	5	**15**
ยุทธศาสตร์ที่ 3: การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์	**กลยุทธ์ที่ 1:** การขับเคลื่อนนโยบายและพัฒนากฎหมายให้ทันสมัยต่อภัยคุกคามทางไซเบอร์	25	7	25	**57**

ยุทธศาสตร์	กลยุทธ์	งบประมาณ (ล้านบาท)			
		2568	2569	2570	รวม
(Empowering the Foundation of Cybersecurity)					
	กลยุทธ์ที่ 2: การผลักดันให้เกิดกลไกการคุ้มครองเด็กออนไลน์ (Child Online Protection) ที่สอดคล้องกับระดับสากล	1	1	1	**3**
	กลยุทธ์ที่ 3: การยกระดับศักยภาพและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์	12.5	7.5	15.5	**35.5**
ยุทธศาสตร์ที่ 4: การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)	**กลยุทธ์ที่ 1:** การส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์	22	22	17	**61**
	กลยุทธ์ที่ 2: การยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์	93	40	40	**173**

ตารางที่ 10 สรุปงบประมาณโครงการในแต่ละปี จำแนกตามยุทธศาสตร์และกลยุทธ์

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
ยุทธศาสตร์ที่ 1 การเพิ่มขีดความสามารถและพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Enhancing Capabilities and Cybersecurity Proficiency)						
กลยุทธ์ที่ 1: การส่งเสริมและสนับสนุนให้บุคลากรทุกระดับในประเทศมีความเข้าใจและตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์						
โครงการ 1.1 โครงการผลักดันความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาศักยภาพบุคลากรระดับชาติ	90	90	90	270	1. มีโปรแกรมการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรระดับชาติที่กำหนดเป้าหมายสำหรับกลุ่มเป้าหมายที่แตกต่างกัน ได้แก่ ผู้บังคับใช้กฎหมาย ผู้ทำหน้าที่ตุลาการ MSMEs หน่วยงานภาคเอกชน หน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ เด็กและเยาวชน และผู้ให้การศึกษา กลุ่มละไม่น้อยกว่า 1 โปรแกรม	**หลัก:** สกมช. (สวม.) **รอง:** สพร./ สพธอ./ สดช./ สอศ./ สพฐ./ อว./ ดศ./ ตร./ สสว./ ปค./ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
					2. มีแพลตฟอร์มในการเผยแพร่และประชาสัมพันธ์โปรแกรมการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์	
โครงการ 1.2 โครงการเสริมสร้างความเข้าใจและตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติ	8	8	8	24	1. มีกิจกรรมหรือแคมเปญการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับกลุ่มเป้าหมายที่แตกต่างกัน ได้แก่ ประชาชนทั่วไป หน่วยงานภาครัฐ ภาคเอกชน MSMEs ภาคประชาสังคม เด็กและเยาวชน ผู้ปกครอง ผู้สูงอายุ และผู้พิการ กลุ่มละไม่น้อยกว่า 1 กิจกรรม 2. มีแพลตฟอร์มในการเผยแพร่และประชาสัมพันธ์กิจกรรมหรือแคมเปญการสร้างความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์	**หลัก:** สกมช. (สวม.) **รอง:** สพร./ สพธอ./ สดช./ สอศ./ สพฐ./ อว./ ดศ./ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
โครงการ 1.3 โครงการฝึกซ้อมแนวทางปฏิบัติเพื่อรับมือภัยคุกคามทางไซเบอร์ในระดับวิกฤตในประเทศ	60	12	12	84	มีการจัดกิจกรรมการฝึกซ้อมแนวทางปฏิบัติเพื่อรับมือภัยคุกคามทางไซเบอร์ปีละไม่น้อยกว่า 1 ครั้ง	**หลัก:** สกมช. (สบพ.) **รอง:** หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
กลยุทธ์ที่ 2: การส่งเสริม สนับสนุน และพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในประเทศ						
โครงการ 1.4 โครงการผลักดัน ส่งเสริมและสนับสนุนการพัฒนาหลักสูตรการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์	6	6	6	18	1. มีกรอบการบูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์เฉพาะทางในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษา มัธยมศึกษา อุดมศึกษา ประกาศนียบัตรวิชาชีพ (ปวช.) และประกาศนียบัตรวิชาชีพชั้นสูง (ปวส.) 2. มีการจัดประชุมร่วมกับหน่วยงานที่เกี่ยวข้องเพื่อผลักดันให้เกิดการพัฒนา	**หลัก**: สกมช. (ศวจ.) **รอง:** สำนักงาน ก.พ./ สคช./ สดช./ สอศ./ สพฐ./ ศธ./ สช./ อว./ ดศ./ บก./ ทท./ สปท./ สำนักงบประมาณ/ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงาน

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
					หลักสูตรการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ ปีละไม่น้อยกว่า 2 ครั้ง	โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
โครงการ 1.5 โครงการส่งเสริมและสนับสนุนการรับรองหลักสูตรวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์	10	-	-	10	1. มีเครื่องมือในการรับรองวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ 2. มีการจัดประชุมร่วมกับหน่วยงานที่เกี่ยวข้องเพื่อผลักดันให้เกิดการรับรองวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ปีละไม่น้อยกว่า 2 ครั้ง	**หลัก:** สกมช. (สวม.)/ กพร./ สคช. **รอง:** สพร./ สพธอ./ อว./ สำนักงาน ก.พ./ สดช./ สอศ./ สพฐ./ ดศ./ สำนักงบประมาณ
โครงการ 1.6 โครงการส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) แก่ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์	5	5	-	10	1. มีใบรับรอง (Certification) สำหรับบุคลากรที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ 2. มีหลักสูตรหรือโปรแกรมการฝึกอบรมสำหรับการรับรองความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์	**หลัก:** สกมช. (ศวจ.)/ สคช. **รอง:** สพร./ สพธอ./ ดศ./ สำนักงาน ก.พ./ สคช./ อว./ สอศ./ บก./ ทท./ สปท./ บีโอไอ/ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงาน

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
						โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ยุทธศาสตร์ที่ 2 การบูรณาการความร่วมมือกับทุกภาคส่วนเพื่อรับมือภัยคุกคามทางไซเบอร์ (Integrating collaboration to confront cybersecurity threats)						
กลยุทธ์ที่ 1: การบูรณาการความร่วมมือเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์						
โครงการ 2.1 โครงการบูรณาการความร่วมมือระหว่างประเทศเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย	15	15	15	45	มีการสนับสนุนความร่วมมือหรือเข้าร่วมโครงการ/กิจกรรมสำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาค ASEAN หรือระดับนานาชาติ ปีละไม่น้อยกว่า 3 ครั้ง	**หลัก:** สกมช. (สปส.) **รอง:** สพร./ สพธอ./ กต./ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
โครงการ 2.2 โครงการบูรณาการความร่วมมือระหว่างหน่วยงานภาครัฐเพื่อเสริมสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ	30	30	30	90	1. มีการสนับสนุนความร่วมมือหรือเข้าร่วมโครงการ/กิจกรรมสำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัย	**หลัก:** สกมช. (ศวจ.) **รอง:** สพร./ สพธอ./ ตร./ ยธ./ กห./ บก./ ทท./ สำนักอัยการสูงสุด (อส.)/

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
					ไซเบอร์ ร่วมกับหน่วยงานภาครัฐในประเทศ ปีละไม่น้อยกว่า 2 ครั้ง 2. มีการจัดกิจกรรมพัฒนาการฝึกอบรมเฉพาะสำหรับการดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ ปีละไม่น้อยกว่า 2 ครั้ง	หน่วยงานควบคุมหรือกำกับดูแล
โครงการ 2.3 โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย	45	45	45	135	มีการสนับสนุนความร่วมมือหรือเข้าร่วมโครงการ/กิจกรรมสำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ร่วมกับหน่วยงานเอกชนในประเทศ ปีละไม่น้อยกว่า 3 ครั้ง	**หลัก:** สกมช. (สปส./ศวจ.) **รอง:** สพร./ สพธอ./ ตร./ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
กลยุทธ์ที่ 2: การประสานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์						
โครงการ 2.4 โครงการจัดประชุมภาคีเครือข่ายเพื่อส่งเสริมการพัฒนาความร่วมมือทางอาญา	5	5	5	15	มีการจัดประชุมเพื่อผลักดันการพัฒนาความร่วมมือทางอาญาระหว่างประเทศ	**หลัก:** สกมช. (สกม.)

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
ระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์					ด้านความมั่นคงปลอดภัยไซเบอร์ ปีละไม่น้อยกว่า 1 ครั้ง	**รอง:** สำนักอัยการสูงสุด (อส.)/ กต./ สคก.
ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Empowering the Foundation of Cybersecurity)						
กลยุทธ์ที่ 1: การขับเคลื่อนนโยบายและพัฒนากฎหมายให้ทันสมัยต่อภัยคุกคามทางไซเบอร์						
โครงการ 3.1 โครงการผลักดันการทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านอาชญากรรมไซเบอร์	5	5	5	15	มีการทบทวนกฎหมายและระเบียบที่เกี่ยวข้องด้านอาชญากรรมไซเบอร์ร่วมกับหน่วยงานที่เกี่ยวข้อง ปีละไม่น้อยกว่า 1 ครั้ง	**หลัก:** สกมช. (สปบ.)/ ดศ. **รอง:** ยธ./ สพร./ สพธอ./ สคส./ หน่วยงานควบคุมหรือกำกับดูแล
โครงการ 3.2 โครงการทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์	15	-	15	30	มีการทบทวนกฎหมายและระเบียบที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ร่วมกับหน่วยงานที่เกี่ยวข้อง ปีละไม่น้อยกว่า 1 ครั้ง	**หลัก:** สกมช. (สกม.) **รอง:** สคส./ ยธ./ กห./ ตร./ สพร/. สพธอ./ หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
โครงการ 3.3 โครงการติดตาม ทบทวนและปรับปรุงนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ประจำปี	5	2	5	12	1. มีการทบทวน แก้ไข หรือปรับปรุงนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ปีละไม่น้อยกว่า 1 ครั้งโดยมีผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญของหน่วยงานของรัฐที่ไม่ใช่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ 2. มีการจัดทำนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับใหม่ (พ.ศ. 2571 - 2575)	**หลัก:** สกมช. (สยศ.) **รอง:** หน่วยงานของรัฐ/ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
กลยุทธ์ที่ 2: การผลักดันให้เกิดกลไกการคุ้มครองเด็กออนไลน์ (Child Online Protection) ที่สอดคล้องกับระดับสากล						

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
โครงการ 3.4 โครงการผลักดัน พัฒนากฎหมายคุ้มครองเด็กออนไลน์ (Child Online Protection Act)	0.5	0.5	0.5	1.5	มีการจัดประชุมเพื่อผลักดันให้เกิดกฎหมายคุ้มครองเด็กออนไลน์ (Child Online Protection Act) ปีละไม่น้อยกว่า 2 ครั้ง	**หลัก:** สกมช. (สกม.)/ ดย. **รอง:** พม./ สคก./ ดศ./ ศธ./ มูลนิธิอินเทอร์เน็ตร่วมพัฒนาไทย
โครงการ 3.5 โครงการความร่วมมือเพื่อทบทวน พัฒนา และปรับปรุง แผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. 2566 - 2570	0.5	0.5	0.5	1.5	มีการจัดประชุมเพื่อทบทวน พัฒนา และปรับปรุง แผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. 2566 - 2570 ปีละไม่น้อยกว่า 2 ครั้ง	**หลัก:** สกมช. (สยศ./สกม.)/ ดย. **รอง:** พม./ สคก./ ยธ./ ดศ./ ศธ./ มูลนิธิอินเทอร์เน็ตร่วมพัฒนาไทย
กลยุทธ์ที่ 3: การยกระดับศักยภาพและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์						
โครงการ 3.6 โครงการพัฒนากรอบการดำเนินงานระดับชาติด้านมาตรฐานความมั่นคงปลอดภัยไซเบอร์	5	-	5	10	มีกรอบการดำเนินงานระดับชาติด้านมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับมาตรฐานสากล	**หลัก:** สกมช. (สบพ.) **รอง:** สพร./ สพธอ./ หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
โครงการ 3.7 โครงการจัดทำกรอบการประเมินศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ (Cybersecurity Self-Assessment)	7.5	7.5	7.5	22.5	1. มีกรอบการประเมินศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นทางการภายในปี พ.ศ 2568 2. มีการทบทวน (ร่าง) แบบประเมินสถานภาพการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ปีละไม่น้อยกว่า 1 ครั้ง	**หลัก:** สกมช. (สบพ.) **รอง**: หน่วยงานของรัฐ/ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
โครงการ 3.8 โครงการส่งเสริมการประเมินและให้การรับรองมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ของผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร	-	-	3	3	มีเครื่องหมายหรือสัญลักษณ์มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร	**หลัก:** สกมช. (ศวจ.)/ DEPA **รอง:** สมอ./ส.อ.ท./ สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์/

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
						สมาคมความมั่นคงปลอดภัยสารสนเทศ
ยุทธศาสตร์ที่ 4 การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)						
กลยุทธ์ที่ 1: การส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์						
โครงการ 4.1 โครงการส่งเสริมและสนับสนุนทุนการวิจัยและพัฒนา นวัตกรรม และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์	15	15	15	45	1. มีศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ภายในปี 2570 2. มีการสนับสนุนทุนการศึกษาวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ปีละไม่น้อยกว่า 3 ทุน หรือมูลค่ารวมไม่น้อยกว่า 10 ล้านบาท	**หลัก:** สกมช. (ศวจ.) **รอง:** หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ/ สพร./

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
						สพธอ./ สำนักงาน ก.พ./ สดช./ สอศ./ สพฐ./ อว./วช./ สวทช./ สทป./ บก./ ทท./ บีโอไอ / NIA
โครงการ 4.2 โครงการประสานความร่วมมือกับสถาบันการศึกษาเพื่อวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์	5	5	-	10	มีการวิจัยและพัฒนานวัตกรรมและเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ภายใต้การดำเนินงานของสถาบันการศึกษาในประเทศ ภายในปี พ.ศ. 2569	**หลัก:** สกมช. (ศวจ.)/ สวทช./ NECTEC **รอง:** ศธ./ อว./ วช./ สถาบันการศึกษา
โครงการ 4.3 โครงการส่งเสริม และสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ	2	2	2	6	มีเครื่องมือหรือกิจกรรมส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ	**หลัก:** สกมช. (ศวจ.) **รอง:** หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ/ สพร./ สพธอ./ สำนักงาน ก.พ./ สคช./ สดช./

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
						สอศ./ สพฐ./ อว./ ดศ./ สทป./ บก./ ทท./ บีโอไอ / ธปท./ ส.อ.ท./ สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
กลยุทธ์ที่ 2: การยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์						
โครงการ 4.4 โครงการยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT)	23	10	10	43	1. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT) เข้าร่วมเป็นสมาชิกของ FIRST และ APCERT ภายในปี พ.ศ. 2568 2. ThaiCERT สามารถคงสภาพการเป็นสมาชิกของ FIRST และ APCERT ได้สำหรับปี พ.ศ. 2569 - 2570	**หลัก:** สกมช. (สปบ.)/ ThaiCERT

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
โครงการ 4.5 โครงการยกระดับการดำเนินการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)	10	10	10	30	1. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) ทั้ง 7 ด้าน มีการดำเนินภารกิจการประสานงาน การเฝ้าระวังภัยคุกคามทางไซเบอร์ การรับมือและแก้ไขภัยคุกคามทางไซเบอร์ และมาตรการด้านการบริหารจัดการคุณภาพ ตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยสมบูรณ์ครบถ้วน 2. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญ	**หลัก:** สกมช. (สปส.) **รอง:** หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
					ทางสารสนเทศ (Sectoral CERT) ได้เข้าร่วมเป็นสมาชิกของ FIRST หรือ APCERT ไม่น้อยกว่า 3 Sector ภายในปี พ.ศ. 2570	
โครงการ 4.6 โครงการสนับสนุนการเผยแพร่และประชาสัมพันธ์กิจกรรมการดำเนินงานของหน่วยงานควบคุมหรือกำกับดูแล และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)	40	-	-	40	1. มีการจัดทำแพลตฟอร์มที่รวบรวมข้อมูล เผยแพร่ และประชาสัมพันธ์กิจกรรม/การดำเนินงานของหน่วยงานควบคุมหรือกำกับดูแล หรือศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) 2.มีกิจกรรมการทำงานร่วมกัน ระหว่างศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับ	**หลัก:** สกมช. (สปส.)/ศูนย์ประสานความมั่นคงปลอดภัยระบบสารสนเทศ (Sectoral CERT) **รอง:** หน่วยงานควบคุมหรือกำกับดูแล

โครงการ	งบประมาณรายปี (ล้านบาท)			งบประมาณรวม (ล้านบาท)	ตัวชี้วัด	หน่วยงานรับผิดชอบ
	68	69	70			
					หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) กับ หน่วยงานภายใน Sector	
โครงการ 4.7 โครงการพัฒนาแพลตฟอร์มสำหรับการแลกเปลี่ยนเหตุการณ์ภัยคุกคามทางไซเบอร์	20	20	20	60	1. มีการจัดทำแพลตฟอร์มสำหรับการรายงานและการแบ่งปันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ 2. ดำเนินการเชื่อมต่อระบบ MISP กับหน่วยงานเพื่อแลกเปลี่ยนข้อมูลแบบอัตโนมัติ เพิ่มขึ้นอย่างน้อยปีละ 10 หน่วยงาน	**หลัก:** สกมช. (สปส.)

ตารางที่ 11 โครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทยระยะ 3 ปี

2.1 โครงการภายใต้ยุทธศาสตร์ที่ 1

ยุทธศาสตร์ที่ 1 การเพิ่มขีดความสามารถและพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Enhancing Capabilities and Cybersecurity Proficiency)	
กลยุทธ์	**โครงการ**
กลยุทธ์ที่ 1: การส่งเสริมและสนับสนุนให้บุคลากรทุกระดับในประเทศมีความเข้าใจและตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์	**โครงการ 1.1** โครงการผลักดันความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาศักยภาพบุคลากรระดับชาติ **โครงการ 1.2** โครงการเสริมสร้างความเข้าใจและตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติ **โครงการ 1.3** โครงการฝึกซ้อมแนวทางปฏิบัติเพื่อรับมือภัยคุกคามทางไซเบอร์ในระดับวิกฤตในประเทศ
กลยุทธ์ที่ 2: การส่งเสริม สนับสนุน และพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในประเทศ	**โครงการ 1.4** โครงการผลักดัน ส่งเสริมและสนับสนุนการพัฒนาหลักสูตรการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ **โครงการ 1.5** โครงการส่งเสริมและสนับสนุนการรับรองหลักสูตรวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ **โครงการ 1.6** โครงการส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) แก่ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

ตารางที่ 12 โครงการภายใต้ยุทธศาสตร์ที่ 1

2.1.1 โครงการผลักดันความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาศักยภาพบุคลากรระดับชาติ

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 1 การเพิ่มขีดความสามารถและพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Enhancing Capabilities and Cybersecurity Proficiency)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 1 การส่งเสริมและสนับสนุนให้บุคลากรทุกระดับในประเทศมีความเข้าใจและตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)</td><td>ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 1.2
โครงการสร้างความตระหนักรู้ระดับชาติสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) และหลากหลายรูปแบบ</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td>ยุทธศาสตร์ที่ 3 กลยุทธ์ที่ 7
โครงการพัฒนาทักษะและขีดความสามารถแก่ประชาชน (กิจกรรมที่ 2.3)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านการพัฒนาศักยภาพ (Capacity Development Measure) ข้อ 2</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรระดับชาติ</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (สวม.)
รอง: สพร./ สพธอ./ สดช./ สอศ./ สพฐ./ อว./ ดศ./ ตร./ สสว./ ปค./หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">3 ปี (ดำเนินการต่อเนื่องทุกปี)</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">270,000,000 บาท</td></tr>
<tr><td>แนวทางการดำเนินงาน</td><td colspan="2">1. จัดทำกรอบโปรแกรมการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรที่กำหนดเป้าหมายสำหรับกลุ่มเป้าหมายที่แตกต่างกัน ได้แก่ MSMEs หน่วยงานภาครัฐ หน่วยงานภาคเอกชน หน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ</td></tr>
</table>

	ผู้ทำหน้าที่ตุลาการ ผู้บังคับใช้กฎหมาย เด็กและเยาวชน และผู้ให้การศึกษา โดยมีกิจกรรมแยกอย่างเฉพาะเจาะจงในแต่ละกลุ่มเป้าหมาย 2. จัดทำหลักสูตรและเนื้อหาโปรแกรมการศึกษาที่กำหนดเป้าหมายสำหรับกลุ่มเป้าหมายที่แตกต่างกัน 3. ประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น ก.พ.ร สำนักงานสถิติแห่งชาติ กระทรวงแรงงาน เป็นต้น ในการกำหนดกรอบและเป้าหมายของโปรแกรมการศึกษาและหารือประเด็นเรื่องการสำรวจความต้องการแรงงานด้านไซเบอร์ของแต่ละหน่วยงาน 4. จัดกิจกรรมส่งเสริม เผยแพร่ โปรแกรมการศึกษาผ่านช่องทางที่หลากหลายตรงกับกลุ่มเป้าหมายเช่น ประชาสัมพันธ์หน่วยงาน โรงเรียน สื่อออนไลน์หรือสื่ออื่น ๆ เป็นต้น 5. พัฒนาแพลตฟอร์ม E-Learning ที่ใช้ในการเผยแพร่โปรแกรมการศึกษาให้มีการระบุกลุ่มเป้าหมายที่แตกต่างกันอย่างชัดเจน 6. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	1. มีโปรแกรมการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรระดับชาติที่กำหนดเป้าหมายสำหรับกลุ่มเป้าหมายที่แตกต่างกัน ได้แก่ ผู้บังคับใช้กฎหมาย ผู้ทำหน้าที่ตุลาการ MSMEs หน่วยงานภาคเอกชน หน่วยงานภาครัฐ หน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ เด็กและเยาวชน และผู้ให้การศึกษา กลุ่มละไม่น้อยกว่า 1 โปรแกรม 2. มีแพลตฟอร์มในการเผยแพร่และประชาสัมพันธ์โปรแกรมการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์

ตารางที่ 13 รายละเอียดของโครงการผลักดันความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาศักยภาพบุคลากรระดับชาติ

2.1.2 โครงการเสริมสร้างความเข้าใจและตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติ

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 1 การเพิ่มขีดความสามารถและพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Enhancing Capabilities and Cybersecurity Proficiency)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 1 การส่งเสริมและสนับสนุนให้บุคลากรทุกระดับในประเทศมีความเข้าใจและตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)</td><td>ยุทธศาสตร์ 1 กลยุทธ์ 1.2
โครงการสร้างความตระหนักรู้ระดับชาติสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) และหลากหลายรูปแบบ</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td>ยุทธศาสตร์ที่ 3 กลยุทธ์ที่ 7
โครงการเสริมสร้างความเข้าใจและสร้างความตระหนักรู้ให้กับประชาชน (กิจกรรมที่ 1.1 และ 1.2)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านการพัฒนาศักยภาพ (Capacity Development Measure) ข้อ 1</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อส่งเสริมและสนับสนุนให้ประชาชนทุกภาคส่วนมีความรู้ ความเข้าใจ และตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (สวม.)
รอง: สพร./ สพธอ./ สดช./ สอศ./ สพฐ./ อว./ ดศ./ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">3 ปี (ดำเนินการต่อเนื่องทุกปี)</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">24,000,000 บาท</td></tr>
<tr><td>แนวทางการดำเนินงาน</td><td colspan="2">1. จัดทำกรอบกิจกรรมหรือแคมเปญการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติด้วยกิจกรรมหรือแคมเปญที่กำหนดเป้าหมายสำหรับกลุ่มเป้าหมายที่แตกต่างกัน ได้แก่ หน่วยงานภาครัฐ ภาคเอกชน</td></tr>
</table>

	MSMEs ภาคประชาสังคม ประชาชนทั่วไป เด็กและเยาวชน ผู้ปกครอง ผู้สูงอายุและผู้พิการ 2. จัดทำเนื้อหากิจกรรมหรือแคมเปญการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ที่กำหนดเป้าหมายสำหรับกลุ่มเป้าหมายที่แตกต่างกัน 3. จัดกิจกรรมส่งเสริม เผยแพร่กิจกรรมหรือแคมเปญการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติ ผ่านช่องทางที่หลากหลายให้ตรงกับแต่ละกลุ่มเป้าหมาย เช่น ละคร โฆษณา การ์ตูน เพลง หรือสื่ออื่น ๆ รวมถึงการให้รางวัลผู้เข้าร่วมกิจกรรม 4. พัฒนาแพลตฟอร์มในการเผยแพร่ ประชาสัมพันธ์กิจกรรมหรือแคมเปญการสร้างความตระหนักรู้ระดับชาติ 5. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	1. มีกิจกรรมหรือแคมเปญการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับกลุ่มเป้าหมายที่แตกต่างกัน ได้แก่ ประชาชนทั่วไป หน่วยงานภาครัฐ ภาคเอกชน MSMEs ภาคประชาสังคม เด็กและเยาวชน ผู้ปกครอง ผู้สูงอายุ และผู้พิการ กลุ่มละไม่น้อยกว่า 1 กิจกรรม 2. มีแพลตฟอร์มในการเผยแพร่และประชาสัมพันธ์กิจกรรมหรือแคมเปญการสร้างความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์

ตารางที่ 14 รายละเอียดของโครงการเสริมสร้างความเข้าใจและตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติ

2.1.3 โครงการฝึกซ้อมแนวทางปฏิบัติเพื่อรับมือภัยคุกคามทางไซเบอร์ในระดับวิกฤตในประเทศ

ยุทธศาสตร์ที่ 1 การเพิ่มขีดความสามารถและพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Enhancing Capabilities and Cybersecurity Proficiency)	
กลยุทธ์ที่ 1 การส่งเสริมและสนับสนุนให้บุคลากรทุกระดับในประเทศมีความเข้าใจและตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์	
ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)	**ยุทธศาสตร์ 1 กลยุทธ์ 1.2** โครงการฝึกซ้อมเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ของประเทศ กิจกรรมการจัดการฝึกและทดสอบแผนเผชิญเหตุในกรณี เกิดเหตุภัยคุกคามทางไซเบอร์ ในระดับวิกฤติ ในประเทศ
ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)	**ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 5** โครงการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ (กิจกรรมที่ 4.1)
Gap GCI Index	ด้านมาตรการทางเทคนิค (Technical Measure) ข้อ 1.2.2 และ 2.2.2
วัตถุประสงค์	เพื่อส่งเสริมและสนับสนุนการเตรียมรับมือภัยคุกคามทางไซเบอร์ในระดับวิกฤตในประเทศ
หน่วยงานที่รับผิดชอบ	**หลัก:** สกมช. (สบพ.) **รอง:** หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ระยะเวลา	3 ปี (ดำเนินการต่อเนื่องทุกปี)
งบประมาณ	84,000,000 บาท
แนวทางการดำเนินงาน	1. กำหนดกรอบแนวทางปฏิบัติเพื่อเตรียมรับมือภัยคุกคามทางไซเบอร์ที่ครอบคลุมทุกรูปแบบ

	2. จัดทำแนวทางปฏิบัติเพื่อเตรียมรับมือภัยคุกคามทางไซเบอร์สำหรับหน่วยงานภาครัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ 3. จัดประชุมวางแผนการฝึก (Exercise Planning) 4. จัดการประชุมเพื่อจัดทำสถานการณ์และโจทย์ฝึก (Exercise Development) 5. จัดกิจกรรมการฝึกซ้อมแนวทางปฏิบัติเพื่อรับมือภัยคุกคามทางไซเบอร์สำหรับทุกกลุ่มเป้าหมาย 6. จัดทำรายงานสรุปผลการฝึก 7. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	มีการจัดกิจกรรมการฝึกซ้อมแนวทางปฏิบัติเพื่อรับมือภัยคุกคามทางไซเบอร์ปีละไม่น้อยกว่า 1 ครั้ง

ตารางที่ 15 รายละเอียดของโครงการฝึกซ้อมแนวทางปฏิบัติเพื่อรับมือภัยคุกคามทางไซเบอร์ ในระดับวิกฤต ในประเทศ

2.1.4 โครงการผลักดัน ส่งเสริมและสนับสนุนการพัฒนาหลักสูตรการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ที่ 1 การเพิ่มขีดความสามารถและพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Enhancing Capabilities and Cybersecurity Proficiency)	
กลยุทธ์ที่ 2 การส่งเสริม สนับสนุน และพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในประเทศ	
ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)	**ยุทธศาสตร์ 1 กลยุทธ์ 1.1** โครงการพัฒนาบุคลากรทางไซเบอร์โดยส่งเสริมให้มีสถาบันการศึกษามีหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์เฉพาะทาง
ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)	**ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 3** โครงการส่งเสริมการวิจัย การสร้างองค์ความรู้และเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.2)

Gap GCI Index	ด้านการพัฒนาศักยภาพ (Capacity Development Measure) ข้อ 3.1–3.3
วัตถุประสงค์	เพื่อผลักดันให้เกิดการพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์ในหลักสูตรการศึกษาในทุกระดับชั้น
หน่วยงานที่รับผิดชอบ	**หลัก**: สกมช. (ศวจ.) **รอง:** สำนักงาน ก.พ./ สคช./ สดช./ สอศ./ สพฐ./ ศธ./ สช./ อว./ ดศ./ สำนักงบประมาณ/ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ/ บก./ ทท./ สปท.
ระยะเวลา	3 ปี
งบประมาณ	18,000,000 บาท
แนวทางการดำเนินงาน	1. จัดการประชุมหารือกับหน่วยงานที่เกี่ยวข้องเพื่อจัดทำกรอบบูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์เฉพาะทางในระบบการศึกษา

	อย่างเป็นทางการตั้งแต่ระดับประถมศึกษา ระดับมัธยมศึกษา ระดับอุดมศึกษา ประกาศนียบัตรวิชาชีพ (ปวช.) และประกาศนียบัตรวิชาชีพชั้นสูง (ปวส.) 2. ร่วมมือกับหน่วยงานที่เกี่ยวข้องในการจัดทำหลักสูตรและเนื้อหาทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์เฉพาะทางในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษา ระดับมัธยมศึกษา ระดับอุดมศึกษา ประกาศนียบัตรวิชาชีพ (ปวช.) และประกาศนียบัตรวิชาชีพชั้นสูง (ปวส.) 3. จัดการประชุมเพื่อผลักดันให้เกิดการพัฒนาหลักสูตรการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ โดยสอดแทรกเป็นส่วนหนึ่งของวิชาบูรณาการ วิชาแนะแนว (เช่น จัดทำ Guideline ข้อมูลพื้นฐานของสายอาชีพ) หรือหลักสูตรระยะสั้นสำหรับทุกระดับชั้น 4. สร้างความร่วมมือระหว่างภาคส่วนต่าง ๆ ในการบูรณาการ 5. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	1. มีกรอบการบูรณาการทักษะการรักษาความมั่นคงปลอดภัยไซเบอร์เฉพาะทางในระบบการศึกษาอย่างเป็นทางการตั้งแต่ระดับประถมศึกษา ระดับมัธยมศึกษา ระดับอุดมศึกษา ประกาศนียบัตรวิชาชีพ (ปวช.) และประกาศนียบัตรวิชาชีพชั้นสูง (ปวส.) 2. มีการจัดประชุมร่วมกับหน่วยงานที่เกี่ยวข้องเพื่อผลักดันให้เกิดการพัฒนาหลักสูตรการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ ปีละไม่น้อยกว่า 2 ครั้ง

ตารางที่ 16 รายละเอียดของโครงการผลักดัน ส่งเสริมและสนับสนุนการพัฒนาหลักสูตรการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์

2.1.5 โครงการส่งเสริมและสนับสนุนการรับรองหลักสูตรวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 1 การเพิ่มขีดความสามารถและพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Enhancing Capabilities and Cybersecurity Proficiency)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 2 การส่งเสริม สนับสนุน และพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในประเทศ</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)</td><td>ยุทธศาสตร์ 1 กลยุทธ์ 1.1
โครงการยกระดับวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ยอมรับ</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td>โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านการพัฒนาศักยภาพ (Capacity Development Measure) ข้อ 2.2</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อส่งเสริมและสนับสนุนการรับรองหลักสูตรวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช./ กพร./ สคช.
รอง: สพร./ สพธอ./ สำนักงาน ก.พ./ อว./ สดช./ สอศ./ สพฐ./ ดศ./ สำนักงบประมาณ</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">1 ปี</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">10,000,000 บาท</td></tr>
<tr><td>แนวทางการดำเนินงาน</td><td colspan="2">1. จัดทำกรอบการดำเนินงานรับรองวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์
2. จัดทำหลักสูตรและเนื้อหาสำหรับการรับรองวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์
3. จัดประชุมหารือกับหน่วยงานที่เกี่ยวข้องเพื่อรับรองหลักสูตรวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ และนำหลักสูตรเสนอให้สถาบันคุณวุฒิวิชาชีพหรือ กรมพัฒนาฝีมือแรงงาน สนับสนุนให้การรับรอง
4. สร้างความร่วมมือระหว่างภาคส่วนต่าง ๆ ในการบูรณาการ
5. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง</td></tr>
</table>

ตัวชี้วัดความสำเร็จของโครงการ	1. มีเครื่องมือในการรับรองวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ 2. มีการจัดประชุมร่วมกับหน่วยงานที่เกี่ยวข้องเพื่อผลักดันให้เกิดการรับรองวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ ปีละไม่น้อยกว่า 2 ครั้ง

ตารางที่ 17 รายละเอียดของโครงการส่งเสริมและสนับสนุนการรับรองหลักสูตรวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์

2.1.6 โครงการส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) แก่ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ที่ 1 การเพิ่มขีดความสามารถและพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Enhancing Capabilities and Cybersecurity Proficiency)	
กลยุทธ์ที่ 2 การส่งเสริม สนับสนุน และพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในประเทศ	
ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)	**ยุทธศาสตร์ 1 กลยุทธ์ 1.1** โครงการพัฒนากรอบความสามารถและโปรแกรมการฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์ ส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญในระดับชาติและนานาชาติ
ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI
Gap GCI Index	ด้านการพัฒนาศักยภาพ (Capacity Development Measure) ข้อ 2.1–2.2
วัตถุประสงค์	เพื่อส่งเสริมและสนับสนุนให้มีการรับรองความสามารถของบุคลากรหรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์
หน่วยงานที่รับผิดชอบ	**หลัก:** สกมช. (ศวจ.)/ สคช. **รอง:** สพร./ สพธอ./ สำนักงาน ก.พ./ ดศ./ สคช./ สอศ./ อว./หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานครงสร้างพื้นฐานสำคัญทางสารสนเทศ/ บก./ ทท./ สปท./ บีโอไอ
ระยะเวลา	2 ปี

งบประมาณ	10,000,000 บาท
แนวทางการดำเนินงาน	1. จัดทำกรอบความสามารถและโปรแกรมการฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และสำหรับผู้ที่ไม่ใช่ไอที (non-IT) การออกใบรับรอง (Certification) บุคลากรที่มีความเชี่ยวชาญ 2. พัฒนาหลักสูตรและเนื้อหาสำหรับตอบสนองกรอบความสามารถและโปรแกรมการฝึกอบรม การออกใบรับรอง (Certification) บุคลากรที่มีความเชี่ยวชาญ 3. เผยแพร่ ประชาสัมพันธ์หลักสูตรให้แก่สาธารณะ และประสานงานกับสถาบันคุณวุฒิวิชาชีพเพื่อสนับสนุนการออกใบรับรอง 4. กำหนดให้ใช้กรอบความสามารถและโปรแกรมการฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์สำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์และสำหรับผู้ที่ไม่ใช่ไอที (non-IT) เป็นส่วนหนึ่งในข้อกำหนดจ้างงาน/เลื่อนตำแหน่ง 5. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	1. มีใบรับรอง (Certification) สำหรับบุคลากรที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ 2. มีหลักสูตรหรือโปรแกรมการฝึกอบรมสำหรับการรับรองความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

ตารางที่ 18 รายละเอียดของโครงการส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) แก่ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์

2.2 โครงการภายใต้ยุทธศาสตร์ที่ 2

ยุทธศาสตร์ที่ 2 การบูรณาการความร่วมมือกับทุกภาคส่วนเพื่อรับมือภัยคุกคามทางไซเบอร์ (Integrating collaboration to confront cybersecurity threats)	
กลยุทธ์	**โครงการ**
กลยุทธ์ที่ 1: การบูรณาการความร่วมมือเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์	**โครงการ 2.1** โครงการบูรณาการความร่วมมือระหว่างประเทศเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย **โครงการ 2.2** โครงการบูรณาการความร่วมมือระหว่างหน่วยงานภาครัฐเพื่อเสริมสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ **โครงการ 2.3** โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย
กลยุทธ์ที่ 2: การประสานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์	**โครงการ 2.4** โครงการจัดประชุมภาคีเครือข่ายเพื่อส่งเสริมการพัฒนาความร่วมมือทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์

ตารางที่ 19 โครงการภายใต้ยุทธศาสตร์ที่ 2

2.2.1 โครงการบูรณาการความร่วมมือระหว่างประเทศเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 2 การบูรณาการความร่วมมือกับทุกภาคส่วนเพื่อรับมือภัยคุกคามทางไซเบอร์ (Integrating collaboration to confront cybersecurity threats)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 1: การบูรณาการความร่วมมือเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)</td><td>ยุทธศาสตร์ 2 กลยุทธ์ 2.2
โครงการส่งเสริมและสนับสนุนความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติเพื่อสร้างศักยภาพด้านไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td>ยุทธศาสตร์ 3 กลยุทธ์ 8
โครงการขยายเครือข่ายความร่วมมือหน่วยงานรัฐ เอกชน และองค์กรระหว่างประเทศหรือนานาชาติ (กิจกรรมที่ 1.1)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านความร่วมมือ (Cooperation Measure) ข้อ 1 และ 2</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อส่งเสริมและสนับสนุนให้ประเทศไทยเกิดความร่วมมือระหว่างประเทศที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (สปส.)
รอง: สพร./ สพธอ./ กต./ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">3 ปี (ดำเนินการต่อเนื่องทุกปี)</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">45,000,000 บาท</td></tr>
</table>

แนวทางการดำเนินงาน	1. กำหนดกรอบแนวทางการส่งเสริมความร่วมมือและเข้าร่วมโครงการ/กิจกรรมสำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาค ASEAN หรือระดับนานาชาติ เพื่อพัฒนาศักยภาพด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ 2. จัดทำแนวทางการส่งเสริมความร่วมมือและเข้าร่วมโครงการ/กิจกรรมสำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาค ASEAN หรือระดับนานาชาติ 3. เผยแพร่ ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ 4. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	มีการสนับสนุนความร่วมมือหรือเข้าร่วมโครงการ/กิจกรรมสำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาค ASEAN หรือระดับนานาชาติ ปีละไม่น้อยกว่า 3 ครั้ง

ตารางที่ 20 รายละเอียดของโครงการบูรณาการความร่วมมือระหว่างประเทศเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย

2.2.2 โครงการบูรณาการความร่วมมือระหว่างหน่วยงานภาครัฐเพื่อเสริมสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 2 การบูรณาการความร่วมมือกับทุกภาคส่วนเพื่อรับมือภัยคุกคามทางไซเบอร์ (Integrating collaboration to confront cybersecurity threats)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 1: การบูรณาการความร่วมมือเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)</td><td>ยุทธศาสตร์ 2 กลยุทธ์ 2.1
โครงการสนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับชาติ</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td>ยุทธศาสตร์ 3 กลยุทธ์ 8
โครงการขยายเครือข่ายความร่วมมือหน่วยงานรัฐ เอกชน และองค์กรระหว่างประเทศหรือนานาชาติ (กิจกรรมที่ 1.2)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านความร่วมมือ (Cooperation Measure) ข้อ 5</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อส่งเสริมและสนับสนุนให้เกิดความร่วมมือระหว่างหน่วยงานภาครัฐเพื่อเสริมสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (ศวจ.)
รอง: สพร./ สพธอ./ ตร./ ยธ./ กห./ บก./ ทท. สำนักอัยการสูงสุด (อส.)/ หน่วยงานควบคุมหรือกำกับดูแล</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">3 ปี (ดำเนินการต่อเนื่องทุกปี)</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">90,000,000 บาท</td></tr>
<tr><td>แนวทางการดำเนินงาน</td><td colspan="2">1. กำหนดแนวทางการส่งเสริมความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศ จัดกิจกรรม และเข้าร่วมโครงการ/กิจกรรมสำคัญร่วมกับหน่วยงานภาครัฐในประเทศ</td></tr>
</table>

	2. กำหนดกรอบการดำเนินการร่วมกันในการต่อต้านอาชญากรรมไซเบอร์เฉพาะทาง พัฒนาการฝึกอบรมเฉพาะสำหรับการดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ 3. จัดทำแนวทางตามกรอบการดำเนินงาน 4. เผยแพร่ ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ 5. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	1. มีการสนับสนุนความร่วมมือหรือเข้าร่วมโครงการ/กิจกรรมสำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ร่วมกับหน่วยงานภาครัฐในประเทศ ปีละไม่น้อยกว่า 2 ครั้ง 2. มีการจัดกิจกรรมพัฒนาการฝึกอบรมเฉพาะสำหรับการดำเนินการร่วมกันระหว่างเจ้าหน้าที่ฝ่ายต่าง ๆ ปีละไม่น้อยกว่า 2 ครั้ง

ตารางที่ 21 รายละเอียดของโครงการบูรณาการความร่วมมือระหว่างหน่วยงานภาครัฐเพื่อเสริมสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซบอร์ในระดับชาติ

2.2.3 โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 2 การบูรณาการความร่วมมือกับทุกภาคส่วนเพื่อรับมือภัยคุกคามทางไซเบอร์ (Integrating collaboration to confront cybersecurity threats)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 1: การบูรณาการความร่วมมือเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)</td><td>ยุทธศาสตร์ 2 กลยุทธ์ 2.1
โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อระบุและตอบสนองต่อปัญหาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td>ยุทธศาสตร์ 3 กลยุทธ์ 8
โครงการขยายเครือข่ายความร่วมมือหน่วยงานรัฐ เอกชน และองค์กรระหว่างประเทศหรือนานาชาติ (กิจกรรมที่ 1.1 และ 1.2)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านความร่วมมือ (Cooperation Measure) ข้อ 4</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">ส่งเสริมและสนับสนุนให้เกิดความร่วมมือระหว่างภาครัฐและเอกชนเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (สปส./ศวจ.)
รอง: สพร./ สพธอ./ ตร./ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">3 ปี (ดำเนินการต่อเนื่องทุกปี)</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">135,000,000 บาท</td></tr>
<tr><td>แนวทางการดำเนินงาน</td><td colspan="2">1. กำหนดแนวทางการส่งเสริมความร่วมมือระหว่างภาครัฐและเอกชนภายในประเทศ และเข้าร่วมโครงการ/กิจกรรมสำคัญที่เกี่ยวข้องกับ</td></tr>
</table>

	ความมั่นคงปลอดภัยไซเบอร์ เพื่อระบุและตอบสนองต่อปัญหาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว 2. จัดทำแนวทางการส่งเสริมความร่วมมือกับหน่วยงานเอกชนภายในประเทศและเข้าร่วมโครงการ/กิจกรรมสำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ 3. สนับสนุนการดำเนินงานของหน่วยงานเอกชนที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ 4. เผยแพร่ ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ 5. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	มีการสนับสนุนความร่วมมือหรือเข้าร่วมโครงการ/กิจกรรมสำคัญที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ร่วมกับหน่วยงานเอกชนในประเทศ ปีละไม่น้อยกว่า 3 ครั้ง

ตารางที่ 22 รายละเอียดของโครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย

2.2.4 โครงการจัดประชุมภาคีเครือข่ายเพื่อส่งเสริมการพัฒนาความร่วมมือทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 2 การบูรณาการความร่วมมือกับทุกภาคส่วนเพื่อรับมือภัยคุกคามทางไซเบอร์ (Integrating collaboration to confront cybersecurity threats)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 2: การประสานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)</td><td>โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td>ยุทธศาสตร์ 2 กลยุทธ์ 6
โครงการดำเนินการเพื่อการบังคับใช้กฎหมายในการจัดการและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
(กิจกรรมที่ 2.2)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านความร่วมมือ (Cooperation Measure) ข้อ 3</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อผลักดันการพัฒนาความร่วมมือทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (สกม.)
รอง: สำนักอัยการสูงสุด (อส.)/ กต./ สคก.</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">3 ปี (ดำเนินการต่อเนื่องทุกปี)</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">15,000,000 บาท</td></tr>
<tr><td>แนวทางการดำเนินงาน</td><td colspan="2">1. จัดการประชุมหารือกับหน่วยงานที่เกี่ยวข้อง (เช่น กระทรวงการต่างประเทศ สำนักอัยการสูงสุด) เพื่อทบทวนประเด็นที่เกี่ยวข้องกับการพัฒนาความร่วมมือ</td></tr>
</table>

	ทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์ตามกรอบของดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index) 2. จัดทำกรอบในการทำงานร่วมกับหน่วยงานที่เกี่ยวข้องเพื่อจัดทำแนวทางการส่งเสริมความร่วมมือทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์ตามกรอบของดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index) 3. จัดประชุมภาคีเครือข่าย หน่วยงานที่เกี่ยวข้อง และผู้เชี่ยวชาญ เพื่อผลักดันการพัฒนาความร่วมมือทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์ 4. จัดทำหรือปรับปรุงกฎหมาย กฎระเบียบที่เกี่ยวข้อง 5. กำกับ ติดตาม และสนับสนุนการเพื่อให้เกิดความร่วมมือทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์
ตัวชี้วัดความสำเร็จของโครงการ	มีการจัดประชุมเพื่อผลักดันการพัฒนาความร่วมมือทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์ปีละไม่น้อยกว่า 1 ครั้ง

ตารางที่ 23 รายละเอียดของโครงการจัดประชุมภาคีเครือข่ายเพื่อส่งเสริมการพัฒนาความร่วมมือทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์

2.3 โครงการภายใต้ยุทธศาสตร์ที่ 3

ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Empowering the Foundation of Cybersecurity)	
กลยุทธ์	**โครงการ**
กลยุทธ์ที่ 1: การขับเคลื่อนนโยบายและพัฒนากฎหมายให้ทันสมัยต่อภัยคุกคามทางไซเบอร์	**โครงการ 3.1** โครงการผลักดันการทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านอาชญากรรมไซเบอร์ **โครงการ 3.2** โครงการทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ **โครงการ 3.3** โครงการติดตาม ทบทวนและปรับปรุงนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ประจำปี
กลยุทธ์ที่ 2: การผลักดันให้เกิดกลไกการคุ้มครองเด็กออนไลน์ (Child Online Protection) ที่สอดคล้องกับระดับสากล	**โครงการ 3.4** โครงการผลักดัน พัฒนากฎหมายคุ้มครองเด็กออนไลน์ (Child Online Protection Act) **โครงการ 3.5** โครงการความร่วมมือเพื่อทบทวน พัฒนา และปรับปรุงแผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. 2566 - 2570
กลยุทธ์ที่ 3: การยกระดับศักยภาพและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์	**โครงการ 3.6** โครงการพัฒนากรอบการดำเนินงานระดับชาติด้านมาตรฐานความมั่นคงปลอดภัยไซเบอร์ **โครงการ 3.7** โครงการจัดทำกรอบการประเมินศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ (Cybersecurity Self-Assessment) **โครงการ 3.8** โครงการส่งเสริมการประเมินและให้การรับรองมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ของผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร

ตารางที่ 24 โครงการภายใต้ยุทธศาสตร์ที่ 3

2.3.1 โครงการผลักดันการทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านอาชญากรรมไซเบอร์

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Empowering the Foundation of Cybersecurity)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 1: การขับเคลื่อนนโยบายและพัฒนากฎหมายให้ทันสมัยต่อภัยคุกคามทางไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)</td><td>ยุทธศาสตร์ 3 กลยุทธ์ 3.2
โครงการกฎระเบียบและข้อบังคับที่สนับสนุนทำให้เกิดความมั่นคงปลอดภัยไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td>ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 6
โครงการดำเนินการเพื่อการบังคับใช้กฎหมายในการจัดการและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
(กิจกรรมที่ 2.2)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านกฎหมาย (Legal Measure) ข้อ 1.1.1 – 1.3.2</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านอาชญากรรมไซเบอร์ให้ครอบคลุม ทันสมัย และสอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (สปบ.) / ดศ.
รอง: ยธ./ สพร./ สพธอ./ สคส./ หน่วยงานควบคุมหรือกำกับดูแล</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">3 ปี (ดำเนินการต่อเนื่องทุกปี)</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">15,000,000 บาท</td></tr>
<tr><td>แนวทางการดำเนินงาน</td><td colspan="2">1. จัดประชุมร่วมกับหน่วยงานที่เกี่ยวข้องเพื่อทบทวนกฎหมายและระเบียบที่เกี่ยวข้องด้านอาชญากรรมไซเบอร์ เช่น การเข้าถึงอุปกรณ์/ข้อมูลระบบคอมพิวเตอร์ที่ผิดกฎหมาย การแทรกแซงที่ผิดกฎหมายบนอุปกรณ์/ข้อมูลระบบคอมพิวเตอร์ การควบคุมเนื้อหาออนไลน์ที่เหยียดเชื้อชาติและเกลียดชาวต่างชาติ การคุกคามทางออนไลน์ และการล่วงละเมิดต่อศักดิ์ศรีหรือความซื่อสัตย์ส่วนบุคคล เป็นต้น
2. จัดทำหรือปรับปรุงกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องด้านอาชญากรรมไซเบอร์ให้ทันสมัยสอดคล้องกับสถานการณ์ในปัจจุบันและอนาคต</td></tr>
</table>

	3. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	มีการทบทวนกฎหมายและระเบียบที่เกี่ยวข้องด้านอาชญากรรมไซเบอร์ ร่วมกับหน่วยงานที่เกี่ยวข้อง ปีละไม่น้อยกว่า 1 ครั้ง

ตารางที่ 25 รายละเอียดของโครงการผลักดันการทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านอาชญากรรมไซเบอร์

2.3.2 โครงการทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ **(Empowering the Foundation of Cybersecurity)**		
กลยุทธ์ที่ 1: การขับเคลื่อนนโยบายและพัฒนากฎหมายให้ทันสมัยต่อภัยคุกคามทางไซเบอร์		
ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)		**ยุทธศาสตร์ 4 กลยุทธ์ 4.1** โครงการปรับปรุงกฎหมาย ระเบียบ และข้อบังคับในด้านความมั่นคงปลอดภัยไซเบอร์
ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)		**ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 6** โครงการปรับปรุงพัฒนา พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง (กิจกรรมที่ 1.1)
Gap GCI Index	ด้านกฎหมาย (Legal Measure) ข้อ 2.1 – 2.8	
วัตถุประสงค์	เพื่อทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ให้ครอบคลุม ทันสมัย และสอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต	
หน่วยงานที่รับผิดชอบ	**หลัก:** สกมช. (สกม.) **รอง:** สคส./ ยธ./ กห./ ตร/. สพร/. สพธอ./ หน่วยงานควบคุมหรือกำกับดูแล	

ระยะเวลา	2 ปี (ดำเนินการปี 68 และ 70)
งบประมาณ	30,000,000 บาท
แนวทางการดำเนินงาน	1. ทบทวนกฎหมายและระเบียบที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การคุ้มครองข้อมูลส่วนบุคคล การคุ้มครองความเป็นส่วนตัวของบุคคล การตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์ที่บังคับใช้กับหน่วยงานภาครัฐ กฎระเบียบที่เกี่ยวข้องกับการระบุและปกป้องโครงสร้างพื้นฐานที่สำคัญของชาติ ลายเซ็นอิเล็กทรอนิกส์ และสแปม เป็นต้น 2. จัดทำหรือปรับปรุงกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ให้ครอบคลุม ทันสมัย และสอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต 3. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	มีการทบทวนกฎหมายและระเบียบที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ร่วมกับหน่วยงานที่เกี่ยวข้อง ปีละไม่น้อยกว่า 1 ครั้ง

ตารางที่ 26 รายละเอียดของโครงการทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์

2.3.3 โครงการติดตาม ทบทวน และปรับปรุงนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ประจำปี

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์
(Empowering the Foundation of Cybersecurity)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 1: การขับเคลื่อนนโยบายและพัฒนากฎหมายให้ทันสมัยต่อภัยคุกคามทางไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)</td><td>ยุทธศาสตร์ที่ 4 กลยุทธ์ที่ 4.3
โครงการขับเคลื่อนแผน ยุทธศาสตร์ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี
(พ.ศ. 2566 – 2570)</td><td>ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 1
โครงการการขับเคลื่อนนโยบายและแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.2 – 1.4)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านหน่วยงาน/นโยบาย (Organizational Measure) ข้อ 1</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อทบทวนและปรับปรุงนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ให้ทันสมัยและสอดคล้องกับสถานการณ์ปัจจุบัน</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (สยศ.)
รอง: หน่วยงานของรัฐ/ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">3 ปี (ดำเนินการต่อเนื่องทุกปี)</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">12,000,000 บาท</td></tr>
<tr><td>แนวทางการดำเนินงาน</td><td colspan="2">1. จัดทำกรอบแนวทางการทบทวนและปรับปรุงนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ทันสมัยและสอดคล้องกับสถานการณ์ปัจจุบัน
2. ดำเนินการจัดประชุมสัมมนาเพื่อทบทวนและปรับปรุงนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญของหน่วยงาน</td></tr>
</table>

	ของรัฐที่ไม่ใช่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ 3. เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ 4. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุน อย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	1. มีการทบทวน แก้ไข หรือปรับปรุงนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ปีละไม่น้อยกว่า 1 ครั้งโดยมีผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญของหน่วยงานของรัฐที่ไม่ใช่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ 2. มีการจัดทำนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับใหม่ (พ.ศ. 2571 - 2575)

ตารางที่ 27 รายละเอียดของโครงการติดตาม ทบทวน และปรับปรุงนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ประจำปี

2.3.4 โครงการผลักดัน พัฒนากฎหมายคุ้มครองเด็กออนไลน์ (Child Online Protection Act)

ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ **(Empowering the Foundation of Cybersecurity)**	
กลยุทธ์ที่ 2: การผลักดันให้เกิดกลไกการคุ้มครองเด็กออนไลน์ (Child Online Protection) ที่สอดคล้องกับระดับสากล	
ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI
ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI
Gap GCI Index	ด้านกฎหมาย (Legal Measure) ข้อ 2.9
วัตถุประสงค์	เพื่อผลักดันให้เกิดกฎหมายคุ้มครองเด็กออนไลน์ (Child Online Protection Act)
หน่วยงานที่รับผิดชอบ	**หลัก:** สกมช. (สกม.)/ ดย. **รอง:** พม./ สคก./ ดศ./ ศธ./ มูลนิธิอินเทอร์เน็ตร่วมพัฒนาไทย
ระยะเวลา	3 ปี
งบประมาณ	1,500,000 บาท
แนวทางการดำเนินงาน	1. จัดประชุมหารือกับหน่วยงานที่รับผิดชอบ เพื่อผลักดันให้เกิดกฎหมายคุ้มครองเด็กออนไลน์ (Child Online Protection Act) 2. ทบทวนกฎหมาย กฎระเบียบ และข้อบังคับที่สนับสนุนการปกป้องคุ้มครองเด็กและเยาวชนในการใช้สื่อออนไลน์ เพื่อสนองตอบกับปัญหาการละเมิดเด็กออนไลน์ในปัจจุบัน เช่น การล่อลวง (Child grooming) การแสวงหาประโยชน์ทางเพศ (the online child sexual exploitation : OCSE) และ Digital Exploitation เช่น การฉ้อโกงออนไลน์ การบังคับขู่เข็ญออนไลน์ การสะกดรอยออนไลน์ เป็นต้น 3. ประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้องเพื่อให้เกิดการบังคับใช้กลไกการคุ้มครองเด็กออนไลน์ และติดตามผลของการแก้กฎหมายอาญา ที่อยู่ระหว่างกระบวนการแก้ไขกฎหมาย ตามมาตรา 77

	4. ติดตาม ประเมินผล ส่งเสริมและสนับสนุน อย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	มีการจัดประชุมเพื่อผลักดันให้เกิดกฎหมายคุ้มครองเด็กออนไลน์ (Child Online Protection Act) ปีละไม่น้อยกว่า 2 ครั้ง

ตารางที่ 28 รายละเอียดโครงการผลักดัน พัฒนากฎหมายคุ้มครองเด็กออนไลน์ (Child Online Protection Act)

2.3.5 โครงการความร่วมมือเพื่อทบทวน พัฒนา และปรับปรุง แผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. 2566 - 2570

ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Empowering the Foundation of Cybersecurity)	
กลยุทธ์ที่ 2: การผลักดันให้เกิดกลไกการคุ้มครองเด็กออนไลน์ (Child Online Protection) ที่สอดคล้องกับระดับสากล	
ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI
ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI
Gap GCI Index	ด้านหน่วยงาน/นโยบาย (Organizational Measure) ข้อ 4.1
วัตถุประสงค์	เพื่อผลักดันให้มีการทบทวน พัฒนา และปรับปรุงแผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. 2566 - 2570 ให้ครอบคลุม ทันสมัย และสอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต
หน่วยงานที่รับผิดชอบ	**หลัก:** สกมช. (สยศ. และ สกม.)/ ดย. รอง: พม./ สคก./ ยธ./ ดศ./ ศธ./ มูลนิธิอินเทอร์เน็ตร่วมพัฒนาไทย
ระยะเวลา	3 ปี
งบประมาณ	1,500,000 บาท
แนวทางการดำเนินงาน	1. ทบทวนกฎระเบียบและข้อบังคับที่สนับสนุนการปกป้องคุ้มครองเด็กและเยาวชนในการใช้สื่อออนไลน์ เพื่อสนองตอบกับปัญหาการละเมิดเด็กออนไลน์ในปัจจุบัน เช่น การล่อลวง (Child grooming) การแสวงหาประโยชน์ทางเพศ (the online child sexual exploitation : OCSE) เป็นต้น

	2. จัดประชุมหารือกับหน่วยงานที่รับผิดชอบ เพื่อทบทวน พัฒนา และปรับปรุงแผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. 2566 - 2570 3. ติดตาม ประเมินผล ส่งเสริมและสนับสนุน อย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	มีการจัดประชุมเพื่อทบทวน พัฒนา และปรับปรุง แผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. 2566 - 2570 ปีละไม่น้อยกว่า 2 ครั้ง

ตารางที่ 29 รายละเอียดของโครงการความร่วมมือเพื่อ ทบทวน พัฒนา และปรับปรุง แผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. 2566 - 2570

2.3.6 โครงการพัฒนากรอบการดำเนินงานระดับชาติด้านมาตรฐานความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Empowering the Foundation of Cybersecurity)		
กลยุทธ์ที่ 3: การยกระดับศักยภาพและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์		
ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)		**ยุทธศาสตร์ที่ 3 กลยุทธ์ที่ 3.3** โครงการพัฒนาและบังคับใช้มาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับบริการภาครัฐ
ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)		**ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 5** โครงการมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.1)
Gap GCI Index	ด้านมาตรการทางเทคนิค (Technical Measure) ข้อ 3	
วัตถุประสงค์	เพื่อพัฒนากรอบการดำเนินงานระดับชาติด้านมาตรฐานความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องตามมาตรฐานสากล	
หน่วยงานที่รับผิดชอบ	**หลัก:** สกมช. (สบพ.) **รอง:** สพร./ สพธอ./ หน่วยงานควบคุมหรือกำกับดูแล	
ระยะเวลา	2 ปี (ปี พ.ศ. 2568 และ 2570)	

งบประมาณ	10,000,000 บาท
แนวทางการดำเนินงาน	1. จัดทำมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับการดำเนินงานของหน่วยงานภาครัฐ หน่วยงานเอกชน และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ที่สอดคล้องตามมาตรฐานระดับสากล (เช่น NIST, ISO/IEC 27001, ISO 28000, ISA 62443 เป็นต้น) 2. พัฒนารูปแบบการกำกับดูแลของภาครัฐและภาระความรับผิดชอบ (Adopt a governance model with clear responsibilities) ของหน่วยงานภาครัฐและผู้มีส่วนเกี่ยวข้องในการปกป้องคุ้มครองโครงสร้างพื้นฐานสำคัญ (Critical infrastructures: CIs) และโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CIIs) 3. เผยแพร่ประชาสัมพันธ์ และให้ความรู้ความเข้าใจในการปฏิบัติ 4. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	มีกรอบการดำเนินงานระดับชาติด้านมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับมาตรฐานสากล

ตารางที่ 30 รายละเอียดของโครงการพัฒนากรอบการดำเนินงานระดับชาติด้านมาตรฐานความมั่นคงปลอดภัยไซเบอร์

2.3.7 โครงการจัดทำกรอบการประเมินศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ (Cybersecurity Self-Assessment)

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Empowering the Foundation of Cybersecurity)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 3: การยกระดับศักยภาพและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)</td><td>ยุทธศาสตร์ 4 กลยุทธ์ 4.1
โครงการขับเคลื่อนแผน ยุทธศาสตร์ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์กิจกรรมยกระดับขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Self-Assessment)</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td>ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 5
โครงการมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.3)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านหน่วยงาน/นโยบาย (Organizational Measures) ข้อ 3.3</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อให้ประเทศไทย มีกรอบการประเมินศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นทางการ</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (สบพ.)
รอง: หน่วยงานของรัฐ/ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">3 ปี</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">22,500,000 บาท</td></tr>
<tr><td>แนวทางการดำเนินงาน</td><td colspan="2">1. ศึกษากรอบแนวคิด เครื่องมือหรือตัวแบบจากข้อมูลทุติยภูมิทั้งในและต่างประเทศที่จะใช้ในการประเมินระดับศักยภาพและความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Self-Assessment)</td></tr>
</table>

	2. จัดทำกรอบแนวคิด เครื่องมือหรือตัวแบบในการประเมินระดับศักยภาพและความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่จะใช้กับหน่วยงานของรัฐที่ไม่ใช่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 3. จัดทำแบบสอบถามอิเล็กทรอนิกส์เพื่อใช้ในการประเมินการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Self-Assessment) 4. รวบรวมข้อมูลสถิติและวิเคราะห์ผลการประเมินระดับศักยภาพและความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์ 5. จัดทำรายงานผลการประเมินระดับศักยภาพและความพร้อมในการรักษาความมั่นคงปลอดภัยไซเบอร์
ตัวชี้วัดความสำเร็จของโครงการ	1. มีกรอบการประเมินศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นทางการภายในปี พ.ศ 2568 2. มีการทบทวน (ร่าง) แบบประเมินสถานภาพการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ปีละไม่น้อยกว่า 1 ครั้ง

ตารางที่ 31 รายละเอียดของโครงการจัดทำกรอบการประเมินศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ (Cybersecurity Self-Assessment)

2.3.8 โครงการส่งเสริมการประเมินและให้การรับรองมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ของผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Empowering the Foundation of Cybersecurity)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 3: การยกระดับศักยภาพและมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์</td></tr>
<tr><td>ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)</td><td colspan="2">ยุทธศาสตร์ที่ 4 กลยุทธ์ที่ 4.1
โครงการส่งเสริมและสนับสนุนการรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ</td></tr>
<tr><td>ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td colspan="2">ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 2
โครงการส่งเสริมการให้บริการและอุตสาหกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.1)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านการพัฒนาศักยภาพ (Capacity Development Measure) ข้อ 4.4</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อจัดทำเครื่องหมายหรือสัญลักษณ์รับรองมาตรฐานความปลอดภัยทางไซเบอร์สำหรับผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสารที่ได้รับการยอมรับในระดับประเทศและระดับสากล</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (ศวจ.)/ สำนักงานส่งเสริมเศรษฐกิจดิจิทัล
รอง: สมอ./ส.อ.ท./ สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์/ สมาคมความมั่นคงปลอดภัยสารสนเทศ</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">1 ปี</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">3,000,000 บาท</td></tr>
<tr><td>แนวทางการดำเนินงาน</td><td colspan="2">1. จัดการประชุมหารือกับหน่วยงานที่เกี่ยวข้อง (เช่น สำนักงานส่งเสริมเศรษฐกิจดิจิทัล) เพื่อผลักดันการขยายขอบเขตของการรับรองผลิตภัณฑ์ dSURE ให้ครอบคลุมถึงผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสารมากขึ้น รวมทั้งร่วมกันกำหนดมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสารที่สอดคล้องกับมาตรฐานสากล เช่น ISO/IEC 27004 และ มอก. 62368-1</td></tr>
</table>

	2. จัดทำกรอบการประเมินผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้การรับรองมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ 3. กำหนดเครื่องหมายหรือสัญลักษณ์ที่แสดงถึงมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อคัดกรองคุณภาพและความปลอดภัย 4. จัดตั้งหรือเข้าร่วมคณะทำงานพิจารณาการคัดกรองผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อขอรับตราสัญลักษณ์ที่แสดงถึงมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ 5. ติดตาม ประเมินผล ส่งเสริมและสนับสนุน อย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	มีเครื่องหมายหรือสัญลักษณ์มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์สำหรับผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร

ตารางที่ 32 รายละเอียดของโครงการส่งเสริมการประเมินและให้การรับรองมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ของผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร

2.4 โครงการภายใต้ยุทธศาสตร์ที่ 4

ยุทธศาสตร์ที่ 4 การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)	
กลยุทธ์	**โครงการ**
กลยุทธ์ที่ 1: การส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์	**โครงการ 4.1** โครงการส่งเสริมและสนับสนุนทุนการวิจัยและพัฒนานวัตกรรม และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์ **โครงการ 4.2** โครงการประสานความร่วมมือกับสถาบันการศึกษาเพื่อวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ **โครงการ 4.3** โครงการส่งเสริมและสนับสนุนการพัฒนาธุรกิจโซลูชันและผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ
กลยุทธ์ที่ 2: การยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์	**โครงการ 4.4** โครงการยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT) **โครงการ 4.5** โครงการยกระดับการดำเนินการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) **โครงการ 4.6** โครงการสนับสนุนการเผยแพร่และประชาสัมพันธ์กิจกรรมการดำเนินงานของหน่วยงานควบคุมหรือกำกับดูแลและศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) **โครงการ 4.7** โครงการพัฒนาแพลตฟอร์มสำหรับการแลกเปลี่ยนเหตุการณ์ภัยคุกคามทางไซเบอร์

ตารางที่ 33 โครงการภายใต้ยุทธศาสตร์ที่ 4

2.4.1 โครงการส่งเสริมและสนับสนุนทุนการวิจัยและพัฒนา นวัตกรรม และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ที่ 4 การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)	
กลยุทธ์ที่ 1: การส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์	
ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)	**ยุทธศาสตร์ 1 กลยุทธ์ 1.3** โครงการส่งเสริมและสนับสนุนให้ทุน และจัดทำแพลตฟอร์มการวิจัยและพัฒนานวัตกรรม วิทยาศาสตร์ และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์
ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)	**ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 3** โครงการส่งเสริมการวิจัย การสร้างองค์ความรู้และเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.3)
Gap GCI Index	ด้านการพัฒนาศักยภาพ (Capacity Development Measure) ข้อ 4.2 6.1 และ 6.3
วัตถุประสงค์	เพื่อส่งเสริมและสนับสนุนการวิจัย พัฒนา และสร้างนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศ
หน่วยงานที่รับผิดชอบ	**หลัก:** สกมช. (ศวจ.) **รอง:** สพร./ สพธอ./ สำนักงาน ก.พ./ สดช./ สอศ./ สพฐ./ อว./วช./ สวทช./ สทป./ บก./ ทท./ บีโอไอ / NIA/ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ระยะเวลา	3 ปี
งบประมาณ	45,000,000 บาท
แนวทางการดำเนินงาน	1. จัดตั้งศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ 2. มีการเผยแพร่สมุดปกขาว บอกทิศทางและแนวทางในการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยของประเทศเป็นรายปี และใช้กำหนดทิศทางในการพัฒนาและให้ทุนสนับสนุน

	3. บูรณาการความร่วมมือกับหน่วยงานที่สามารถสนับสนุนทุนวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น กองทุนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม) เพื่อให้ทุนและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรทั่วไป หน่วยงานที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์ นักศึกษา และนักวิจัย 4. ส่งเสริมการทำงานร่วมกัน (Collaboration) รูปแบบการระดมทุน 5. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง 6. เผยแพร่และประชาสัมพันธ์ผลลัพธ์การวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ให้ประชาชนทั่วไปรับทราบ
ตัวชี้วัดความสำเร็จของโครงการ	1. มีศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ ภายในปี 2570 2. มีการสนับสนุนทุนการศึกษาวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ปีละไม่น้อยกว่า 3 ทุน หรือ มูลค่ารวมไม่น้อยกว่า 10 ล้านบาท

ตารางที่ 34 รายละเอียดของโครงการส่งเสริมและสนับสนุนทุนการวิจัยและพัฒนา นวัตกรรม และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์

2.4.2 โครงการประสานความร่วมมือกับสถาบันการศึกษาเพื่อวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์

ยุทธศาสตร์ที่ 4 การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)	
กลยุทธ์ที่ 1: การส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์	
ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI
ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI
Gap GCI Index	ด้านการพัฒนาศักยภาพ (Capacity Development Measure) ข้อ 4.3
วัตถุประสงค์	เพื่อสนับสนุนและส่งเสริมให้เกิดการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันการศึกษาในประเทศ
หน่วยงานที่รับผิดชอบ	**หลัก:** สกมช. (ศวจ.)/ สวทช./ NECTEC **รอง:** ศธ./ อว./ วช./ สถาบันการศึกษาที่เกี่ยวข้อง เช่น MU KMITL KMUTT SPU
ระยะเวลา	2 ปี
งบประมาณ	10,000,000 บาท
แนวทางการดำเนินงาน	1. ประสานความร่วมมือกับสถาบันการศึกษาในประเทศ เพื่อส่งเสริมการวิจัยและพัฒนานวัตกรรมและเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ ภายใต้การดำเนินงานของสถาบันการศึกษา 2. จัดทำกรอบการดำเนินงานส่งเสริมการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ 3. ติดตาม ประเมินผล และสำรวจงานวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ รวมทั้งส่งเสริมและสนับสนุนอย่างต่อเนื่อง 4. เผยแพร่และประชาสัมพันธ์ผลลัพธ์การวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ให้ประชาชนทั่วไปรับทราบ
ตัวชี้วัดความสำเร็จของโครงการ	มีการวิจัยและพัฒนานวัตกรรมและเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์ภายใต้การดำเนินงานของสถาบันการศึกษาในประเทศ ภายในปี พ.ศ. 2569

ตารางที่ 35 รายละเอียดของโครงการประสานความร่วมมือกับสถาบันการศึกษาเพื่อวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์

2.4.3 โครงการส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 4 การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 1: การส่งเสริมและสนับสนุนการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)</td><td>ยุทธศาสตร์ 1 กลยุทธ์ 1.3
โครงการส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td>ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 2
โครงการส่งเสริมการให้บริการและอุตสาหกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.3)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านการพัฒนาศักยภาพ (Capacity Development Measure) ข้อ 6.2</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อผลักดันให้เกิดการสร้างมาตรการจูงใจเพื่อสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (ศวจ.)
รอง: สพร./ สพธอ./ สำนักงาน ก.พ./ สคช./ สดช./ สอศ./ สพฐ./ อว./ ดศ./ สทป./ บก./ ทท./ บีโอไอ / ธปท./ ส.อ.ท./ หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ/ สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">3 ปี</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">6,000,000 บาท</td></tr>
</table>

แนวทางการดำเนินงาน	1. จัดทำนโยบายและแนวทางในการส่งเสริมการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ 2. ให้ความรู้และความร่วมมือกับสตาร์ทอัพด้านความมั่นคงปลอดภัยไซเบอร์ในประเทศไทย โดยร่วมมือกับนักวิจัย มหาวิทยาลัย บริษัทชั้นนำทั้งในและต่างประเทศ 3. สร้างแบรนด์และความน่าเชื่อถือของโซลูชันและผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ 4. ส่งเสริมการใช้โซลูชันและผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ โดยให้สิทธิพิเศษและการสนับสนุนในด้านต่าง ๆ 5. สนับสนุนการมีส่วนร่วม โดยอาจพิจารณาสิทธิพิเศษทางภาษี และมาตรการส่งเสริมต่าง ๆ เพื่อเพิ่มจำนวนของหน่วยงานสนับสนุน 6. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	มีเครื่องมือหรือกิจกรรมส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ

ตารางที่ 36 รายละเอียดของโครงการส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ

2.4.4 โครงการยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT)

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 4 การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 2: การยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)</td><td>โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td>ยุทธศาสตร์ 2 กลยุทธ์ 4
โครงการยกระดับการเฝ้าระวัง ตอบสนอง รับมือและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (กิจกรรมที่ 1.4 และ 1.5)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านมาตรการทางเทคนิค (Technical Measure) ข้อ 1.3 – 1.4</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อยกระดับการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT) ให้ครอบคลุมตามประเด็นดัชนีชี้วัดความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU)</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (สปบ.) / ThaiCERT</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">3 ปี</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">43,000,000 บาท</td></tr>
<tr><td>แนวทางการดำเนินงาน</td><td colspan="2">1. สนับสนุนและส่งเสริมการยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT) เช่น การเพิ่มประสิทธิภาพเครื่องมือทางเทคนิคที่จำเป็น การพัฒนาระบบ</td></tr>
</table>

	เฝ้าระวัง ตรวจจับ รับมือและแก้ปัญหาทางไซเบอร์ การพัฒนาศักยภาพ และทักษะบุคลากร เป็นต้น 2. สนับสนุนและส่งเสริมให้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT) เข้าร่วมเป็นสมาชิกของ APCERT โดยการกำหนดแนวทางการเข้าร่วมเป็นสมาชิกดังกล่าว 3. จัดตั้งคณะทำงานสำหรับประสานงานด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศ 4. กำกับดูแล ติดตามและประเมินผลการดำเนินงานของ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team:ThaiCERT)
ตัวชี้วัดความสำเร็จของโครงการ	1. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT) เข้าร่วมเป็นสมาชิกของ APCERT ภายในปี พ.ศ. 2568 2. ThaiCERT สามารถคงสภาพความเป็นสมาชิกของ FIRST และ APCERT ได้สำหรับปี พ.ศ. 2569 - 2570

ตารางที่ 37 รายละเอียดของโครงการยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT)

2.4.5 โครงการยกระดับการดำเนินการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)

ยุทธศาสตร์ที่ 4 การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)	
กลยุทธ์ที่ 2: การยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์	
ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI
ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI
Gap GCI Index	ด้านมาตรการทางเทคนิค (Technical Measure) ข้อ 2.1
วัตถุประสงค์	เพื่อยกระดับการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) ให้ครอบคลุมตามประเด็นดัชนีชี้วัดความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU)
หน่วยงานที่รับผิดชอบ	**หลัก:** สกมช. (สปส.) **รอง:** หน่วยงานควบคุมหรือกำกับดูแล/ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ระยะเวลา	3 ปี
งบประมาณ	30,000,000 บาท
แนวทางการดำเนินงาน	1. กำหนดกรอบการดำเนินงานร่วมกับ Sectoral CERT และหน่วยงานควบคุมหรือกำกับดูแล 2. สนับสนุนและส่งเสริมให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) สามารถดำเนินภารกิจตามพระราชบัญญัติ ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้แก่ การประสานงาน การเฝ้าระวังภัยคุกคามทางไซเบอร์ การรับมือ

	และแก้ไขภัยคุกคามทางไซเบอร์ และมาตรการด้านการบริหารจัดการคุณภาพผ่านระบบพี่เลี้ยง (Mentoring) หรือการสนับสนุนงบประมาณการดำเนินงาน 3. สนับสนุนและส่งเสริมให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) เข้าร่วมเป็นสมาชิกของ FIRST APCERT ISACs หรือ ISAOs โดยการกำหนดแนวทางการเข้าร่วมเป็นสมาชิกดังกล่าว 4. ติดตามและประเมินผลการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)
ตัวชี้วัดความสำเร็จของโครงการ	1. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) ทั้ง 7 ด้าน มีการดำเนินภารกิจการประสานงาน การเฝ้าระวังภัยคุกคามทางไซเบอร์ การรับมือและแก้ไขภัยคุกคามทางไซเบอร์ และมาตรการด้านการบริหารจัดการคุณภาพ ตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยสมบูรณ์ครบถ้วน 2. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) ได้เข้าร่วมเป็นสมาชิกของ FIRST หรือ APCERT ไม่น้อยกว่า 3 Sector ภายในปี พ.ศ. 2570

ตารางที่ 38 รายละเอียดของโครงการยกระดับการดำเนินการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)

2.4.6 โครงการสนับสนุนการเผยแพร่และประชาสัมพันธ์กิจกรรมการดำเนินงานของหน่วยงานควบคุมหรือกำกับดูแล และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)

<table>
<tr><td colspan="3">ยุทธศาสตร์ที่ 4 การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)</td></tr>
<tr><td colspan="3">กลยุทธ์ที่ 2: การยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์</td></tr>
<tr><td colspan="2">ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)</td><td>โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI</td></tr>
<tr><td colspan="2">ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)</td><td>ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 4
โครงการยกระดับการประสานงานในการตอบสนองและแลกเปลี่ยนข้อมูล ภัยคุกคามทางไซเบอร์ (กิจกรรมที่ 2.3)</td></tr>
<tr><td>Gap GCI Index</td><td colspan="2">ด้านมาตรการทางเทคนิค (Technical Measure) ข้อ 2.2.1</td></tr>
<tr><td>วัตถุประสงค์</td><td colspan="2">เพื่อรวบรวมข้อมูล เผยแพร่และประชาสัมพันธ์ กิจกรรม/การดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)</td></tr>
<tr><td>หน่วยงานที่รับผิดชอบ</td><td colspan="2">หลัก: สกมช. (สปส.)/ ศูนย์ประสานความมั่นคงปลอดภัยระบบสารสนเทศ (Sectoral CERT)
รอง: หน่วยงานควบคุมหรือกำกับดูแล</td></tr>
<tr><td>ระยะเวลา</td><td colspan="2">1 ปี</td></tr>
<tr><td>งบประมาณ</td><td colspan="2">40,000,000 บาท</td></tr>
</table>

แนวทางการดำเนินงาน	1. จัดการประชุมหารือร่วมกัน ระหว่าง สกมช. ThaiCERT Sectoral CERT และหน่วยงานควบคุมหรือกำกับดูแล เพื่อกำหนดแนวทางการดำเนินงาน 2. จัดทำแพลตฟอร์มที่รวบรวมข้อมูล เผยแพร่ และประชาสัมพันธ์กิจกรรม/การดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) 3. ติดตามและประเมินผลการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) 4. รวบรวมข้อมูล เผยแพร่และประชาสัมพันธ์ กิจกรรม/การดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)
ตัวชี้วัดความสำเร็จของโครงการ	1. มีการจัดทำแพลตฟอร์มที่รวบรวมข้อมูล เผยแพร่ และประชาสัมพันธ์กิจกรรม/การดำเนินงานของหน่วยงานควบคุมหรือกำกับดูแล หรือศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) 2. มีกิจกรรมการทำงานร่วมกัน ระหว่าง ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT) กับ หน่วยงานภายใน Sector

ตารางที่ 39 รายละเอียดของโครงการสนับสนุนการเผยแพร่และประชาสัมพันธ์กิจกรรมการดำเนินงานของหน่วยงานควบคุมหรือกำกับดูแล และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)

2.4.7 โครงการพัฒนาแพลตฟอร์มสำหรับการแลกเปลี่ยนเหตุการณ์ภัยคุกคามทางไซเบอร์

ยุทธศาสตร์ที่ 4 การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)	
กลยุทธ์ที่ 2: การยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์	
ความสอดคล้องนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (65-70)	**ยุทธศาสตร์ 4 กลยุทธ์ 4.2** โครงการพัฒนาแพลตฟอร์มสำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์
ความสอดคล้องแผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)	**ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 4** โครงการพัฒนา Platform สำหรับการรับและแบ่งปันเหตุการณ์ไซเบอร์ (ระบบ MISP) (กิจกรรมที่ 4.1)

Gap GCI Index	ด้านมาตรการทางเทคนิค (Technical Measure) ข้อ 2.2.1
วัตถุประสงค์	เพื่อรวบรวมข้อมูล เผยแพร่และประชาสัมพันธ์ กิจกรรม/การดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)
หน่วยงานที่รับผิดชอบ	**หลัก:** สกมช. (สปส.)
ระยะเวลา	3 ปี
งบประมาณ	60,000,000 บาท
แนวทางการดำเนินงาน	1. สร้างกลไกการแบ่งปันข้อมูลระหว่างภาครัฐและเอกชน ระหว่างหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ Sector CERT และหน่วยงานด้านความมั่นคง 2. พัฒนาแพลตฟอร์มสำหรับการรายงานและการแบ่งปัน เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ข้ามภาคส่วน

	3. จัดทำเอกสารเพื่อเป็นแนวทางในการใช้ระบบและ เชื่อมต่อ MISP ไปยังหน่วยงานต่าง ๆ - SOP (Standard operating Procedure) for information sharing -หนังสือข้อตกลงในการใช้และเชื่อมต่อระบบ MISP 4. สร้างความรู้ความเข้าใจถึงการแลกเปลี่ยนข้อมูลตาม SOP 5. ดำเนินการให้สิทธิ์การเข้าใช้ MISP กลาง 6. ดำเนินการออกแบบเตรียม Environment ของ สกมช. เพื่อการเชื่อมต่อ 7. กำกับดูแล ติดตาม ประเมินผล ส่งเสริมและสนับสนุนอย่างต่อเนื่อง
ตัวชี้วัดความสำเร็จของโครงการ	1. มีการจัดทำแพลตฟอร์มสำหรับการรายงานและการแบ่งปันเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ 2. ดำเนินการเชื่อมต่อระบบ MISP กับหน่วยงานเพื่อแลกเปลี่ยนข้อมูลแบบอัตโนมัติเพิ่มขึ้นอย่างน้อยปีละ 10 หน่วยงาน

ตารางที่ 40 รายละเอียดของโครงการพัฒนาแพลตฟอร์มสำหรับการแลกเปลี่ยนเหตุการณ์ภัยคุกคามทางไซเบอร์

2.5 ความเชื่อมโยงของโครงการ

ความเชื่อมโยงของโครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี		
โครงการ	**นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**	**แผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)**
ยุทธศาสตร์ที่ 1 การเพิ่มขีดความสามารถและพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Enhancing Capabilities and Cybersecurity Proficiency)		
โครงการ 1.1 โครงการผลักดันความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อพัฒนาศักยภาพบุคลากรระดับชาติ	**ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 1.2** โครงการสร้างความตระหนักรู้ระดับชาติสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) และหลากหลายรูปแบบ	**ยุทธศาสตร์ที่ 3 กลยุทธ์ที่ 7** โครงการพัฒนาทักษะและขีดความสามารถแก่ประชาชน (กิจกรรรที่ 2.3)
โครงการ 1.2 โครงการเสริมสร้างความเข้าใจและตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ระดับชาติ	**ยุทธศาสตร์ 1 กลยุทธ์ 1.2** โครงการสร้างความตระหนักรู้ระดับชาติสำหรับกลุ่มเป้าหมายที่แตกต่างกัน (เช่น ผู้บริโภคทั่วไป ผู้ใช้ในองค์กร เด็ก ธุรกิจ) และหลากหลายรูปแบบ	**ยุทธศาสตร์ที่ 3 กลยุทธ์ที่ 7** โครงการเสริมสร้างความเข้าใจและสร้างความตระหนักรู้ให้กับประชาชน (กิจกรรมที่ 1.1 และ 1.2)

ความเชื่อมโยงของโครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี		
โครงการ	**นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**	**แผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)**
โครงการ 1.3 โครงการฝึกซ้อมแนวทางปฏิบัติเพื่อรับมือภัยคุกคามทางไซเบอร์ในระดับวิกฤตในประเทศ	**ยุทธศาสตร์ 1 กลยุทธ์ 1.2** โครงการฝึกซ้อมเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ของประเทศ กิจกรรมการจัดการฝึกและทดสอบแผนเผชิญเหตุในกรณี เกิดเหตุภัยคุกคามทางไซเบอร์ ในระดับวิกฤติ ในประเทศ	**ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 5** โครงการฝึกเพื่อทดสอบขีดความสามารถทางไซเบอร์ (กิจกรรมที่ 4.1)
โครงการ 1.4 โครงการผลักดัน ส่งเสริมและสนับสนุนการพัฒนาหลักสูตรการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์	**ยุทธศาสตร์ 1 กลยุทธ์ 1.1** โครงการพัฒนาบุคลากรทางไซเบอร์โดยส่งเสริมให้มีสถาบันการศึกษามีหลักสูตรด้านความมั่นคงปลอดภัยไซเบอร์เฉพาะทาง	**ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 3** โครงการส่งเสริมการวิจัย การสร้างองค์ความรู้และเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.2)

ความเชื่อมโยงของโครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี		
โครงการ	**นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**	**แผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)**
โครงการ 1.5 โครงการส่งเสริมและสนับสนุนการรับรองหลักสูตรวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์	**ยุทธศาสตร์ 1 กลยุทธ์ 1.1** โครงการยกระดับวิชาชีพด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นที่ยอมรับ	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI
โครงการ 1.6 โครงการส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) แก่ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์	**ยุทธศาสตร์ 1 กลยุทธ์ 1.1** โครงการพัฒนากรอบความสามารถและโปรแกรมการฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์ส่งเสริมและสนับสนุนการออกใบรับรอง (Certification) และการรับรอง (Accreditation) บุคลากรที่มีความเชี่ยวชาญในระดับชาติและนานาชาติ	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI
ยุทธศาสตร์ที่ 2 การบูรณาการความร่วมมือกับทุกภาคส่วนเพื่อรับมือภัยคุกคามทางไซเบอร์ (Integrating collaboration to confront cybersecurity threats)		

ความเชื่อมโยงของโครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี		
โครงการ	**นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**	**แผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)**
โครงการ 2.1 โครงการบูรณาการความร่วมมือระหว่างประเทศเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย	**ยุทธศาสตร์ 2 กลยุทธ์ 2.2** โครงการส่งเสริมและสนับสนุนความร่วมมือและเข้าร่วมโครงการสำคัญในระดับ ASEAN และนานาชาติ เพื่อสร้างศักยภาพด้านไซเบอร์	**ยุทธศาสตร์ 3 กลยุทธ์ 8** โครงการขยายเครือข่ายความร่วมมือหน่วยงานรัฐ เอกชน และองค์กรระหว่างประเทศหรือนานาชาติ (กิจกรรมที่ 1.1)
โครงการ 2.2 โครงการบูรณาการความร่วมมือระหว่างหน่วยงานภาครัฐเพื่อเสริมสร้างขีดความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ	**ยุทธศาสตร์ 2 กลยุทธ์ 2.1** โครงการสนับสนุนการสร้างขีดความสามารถด้านอาชญากรรมไซเบอร์ในระดับชาติ	**ยุทธศาสตร์ 3 กลยุทธ์ 8** โครงการขยายเครือข่ายความร่วมมือหน่วยงานรัฐ เอกชน และองค์กรระหว่างประเทศหรือนานาชาติ (กิจกรรมที่ 1.2)

ความเชื่อมโยงของโครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี		
โครงการ	**นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**	**แผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)**
โครงการ 2.3 โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อยกระดับขีดความสามารถในการรับมือภัยคุกคามทางไซเบอร์ของประเทศไทย	**ยุทธศาสตร์ 2 กลยุทธ์ 2.1** โครงการส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชนเพื่อระบุและตอบสนองต่อปัญหาที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว	**ยุทธศาสตร์ 3 กลยุทธ์ 8** โครงการขยายเครือข่ายความร่วมมือหน่วยงานรัฐ เอกชน และองค์กรระหว่างประเทศหรือนานาชาติ (กิจกรรมที่ 1.1 และ 1.2)
โครงการ 2.4 โครงการจัดประชุมภาคีเครือข่ายเพื่อส่งเสริมการพัฒนาความร่วมมือทางอาญาระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI	**ยุทธศาสตร์ 2 กลยุทธ์ 6** โครงการดำเนินการเพื่อการบังคับใช้กฎหมายในการจัดการและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ (กิจกรรมที่ 2.2)
ยุทธศาสตร์ที่ 3 การวางรากฐานด้านความมั่นคงปลอดภัยไซเบอร์ (Empowering the Foundation of Cybersecurity)		

ความเชื่อมโยงของโครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี		
โครงการ	**นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**	**แผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)**
โครงการ 3.1 โครงการผลักดันการทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านอาชญากรรมไซเบอร์	**ยุทธศาสตร์ 3 กลยุทธ์ 3.2** โครงการกฎระเบียบและข้อบังคับที่สนับสนุนทำให้เกิดความมั่นคงปลอดภัยไซเบอร์	**ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 6** โครงการดำเนินการเพื่อการบังคับใช้กฎหมายในการจัดการและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ (กิจกรรมที่ 2.2)
โครงการ 3.2 โครงการทบทวน ปรับปรุง และพัฒนา กฎหมายและระเบียบที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์	**ยุทธศาสตร์ 4 กลยุทธ์ 4.1** โครงการปรับปรุงกฎหมาย ระเบียบ และข้อบังคับในด้านความมั่นคงปลอดภัยไซเบอร์	**ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 6** โครงการปรับปรุงพัฒนา พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง (กิจกรรมที่ 1.1)
โครงการ 3.3 โครงการติดตาม ทบทวนและปรับปรุงนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ประจำปี	**ยุทธศาสตร์ที่ 4 กลยุทธ์ที่ 4.3** โครงการขับเคลื่อนแผน ยุทธศาสตร์ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์	**ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 1** โครงการการขับเคลื่อนนโยบายและแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.2 – 1.4)

ความเชื่อมโยงของโครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี		
โครงการ	**นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**	**แผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)**
โครงการ 3.4 โครงการผลักดัน พัฒนากฎหมายคุ้มครองเด็กออนไลน์ (Child Online Protection Act)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI	
โครงการ 3.5 โครงการความร่วมมือเพื่อทบทวน พัฒนา และปรับปรุง แผนปฏิบัติการด้านการคุ้มครองเด็กแห่งชาติ พ.ศ. 2566 - 2570	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI	
โครงการ 3.6 โครงการพัฒนากรอบการดำเนินงานระดับชาติด้านมาตรฐานความมั่นคงปลอดภัยไซเบอร์	**ยุทธศาสตร์ที่ 3 กลยุทธ์ที่ 3.3** โครงการพัฒนาและบังคับใช้มาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับบริการภาครัฐ	**ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 5** โครงการมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.1)

ความเชื่อมโยงของโครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี		
โครงการ	**นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**	**แผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)**
โครงการ 3.7 โครงการจัดทำกรอบการประเมินศักยภาพและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ (Cybersecurity Self-Assessment)	**ยุทธศาสตร์ 4 กลยุทธ์ 4.1** โครงการขับเคลื่อนแผน ยุทธศาสตร์ นโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์กิจกรรมยกระดับขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Self-Assessment)	**ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 5** โครงการมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.3)
โครงการ 3.8 โครงการส่งเสริมการประเมินและให้การรับรองมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ของผลิตภัณฑ์เทคโนโลยีสารสนเทศและการสื่อสาร	**ยุทธศาสตร์ที่ 4 กลยุทธ์ที่ 4.1** โครงการส่งเสริมและสนับสนุนการรวมผลิตภัณฑ์ความมั่นคงปลอดภัยไซเบอร์เข้ากับข้อเสนอบริการอื่น ๆ	**ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 2** โครงการส่งเสริมการให้บริการและอุตสาหกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.1)
ยุทธศาสตร์ที่ 4 การยกระดับอุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยสู่สากล (Elevating Cybersecurity Industry)		

ความเชื่อมโยงของโครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี		
โครงการ	**นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**	**แผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)**
โครงการ 4.1 โครงการส่งเสริมและสนับสนุนทุนการวิจัยและพัฒนา นวัตกรรม และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์	**ยุทธศาสตร์ 1 กลยุทธ์ 1.3** โครงการส่งเสริมและสนับสนุนให้ทุน และจัดทำแพลตฟอร์มการวิจัยและพัฒนานวัตกรรม วิทยาศาสตร์ และเทคโนโลยีการรักษาความมั่นคงปลอดภัยไซเบอร์	**ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 3** โครงการส่งเสริมการวิจัย การสร้างองค์ความรู้และเทคโนโลยีด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.3)
โครงการ 4.2 โครงการประสานความร่วมมือกับสถาบันการศึกษาเพื่อวิจัยและพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI	
โครงการ 4.3 โครงการส่งเสริมและสนับสนุนการพัฒนาธุรกิจโซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ	**ยุทธศาสตร์ 1 กลยุทธ์ 1.3**	**ยุทธศาสตร์ที่ 1 กลยุทธ์ที่ 2** โครงการส่งเสริมการให้บริการและอุตสาหกรรมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (กิจกรรมที่ 1.3)

ความเชื่อมโยงของโครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี		
โครงการ	**นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**	**แผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)**
	โครงการส่งเสริมและสนับสนุนการพัฒนาธุรกิจ โซลูชัน และผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมในประเทศ	
โครงการ 4.4 โครงการยกระดับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team: ThaiCERT)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI	**ยุทธศาสตร์ 2 กลยุทธ์ 4** โครงการยกระดับการเฝ้าระวัง ตอบสนอง รับมือและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ (กิจกรรมที่ 1.4 และ 1.5)
โครงการ 4.5 โครงการยกระดับการดำเนินการของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI	

ความเชื่อมโยงของโครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี		
โครงการ	**นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**	**แผนปฏิบัติการระยะ 5 ปี (พ.ศ. 2566 – 2570)**
โครงการ 4.6 โครงการสนับสนุนการเผยแพร่และประชาสัมพันธ์กิจกรรมการดำเนินงานของหน่วยงานควบคุมหรือกำกับดูแล และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Sectoral CERT)	โครงการเสนอเพิ่มเติมเพื่อให้สอดคล้อง GCI	**ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 4** โครงการยกระดับการประสานงานในการตอบสนองและแลกเปลี่ยนข้อมูลภัยคุกคามทางไซเบอร์ (กิจกรรมที่ 2.3)
โครงการ 4.7 โครงการพัฒนาแพลตฟอร์มสำหรับการแลกเปลี่ยนเหตุการณ์ภัยคุกคามทางไซเบอร์	**ยุทธศาสตร์ 4 กลยุทธ์ 4.2** โครงการพัฒนาแพลตฟอร์มสำหรับการรับและแบ่งปันเหตุการณ์ภัยคุกคามทางไซเบอร์	**ยุทธศาสตร์ที่ 2 กลยุทธ์ที่ 4** โครงการพัฒนา Platform สำหรับการรับและแบ่งปันเหตุการณ์ไซเบอร์ (ระบบ MISP) (กิจกรรมที่ 4.1)

ตารางที่ 41 ความเชื่อมโยงของโครงการภายใต้ แนวทางการยกระดับดัชนีด้านความมั่นคงปลอดภัยไซเบอร์ (Global Cybersecurity Index: GCI) ของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สำหรับประเทศไทย ระยะ 3 ปี