

รายงานผลการดำเนินงาน ปีงบประมาณ พ.ศ. ๒๕๖๑ (รอบ ๖ เดือนหลัง) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

จากสถานการณ์ปัจจุบันที่มีการใช้งานอินเทอร์เน็ตเพิ่มสูงขึ้นอย่างรวดเร็ว ซึ่งจะเห็นได้จากผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ซึ่งพบว่าในปี พ.ศ. ๒๕๖๑ คนไทยมีการใช้งานอินเทอร์เน็ตเฉลี่ยสูงถึง ๑๐.๕๐ ชั่วโมงต่อวัน เพิ่มขึ้นจากปี พ.ศ. ๒๕๖๐ จำนวน ๓ ชั่วโมง ๔๑ นาที โดยพบว่าปัญหาที่เกิดขึ้นจากการใช้งานอินเทอร์เน็ตเป็นเรื่องของการถูกหลอกลวงและการละเมิดข้อมูลส่วนบุคคล การขาดความมั่นใจและความเชื่อถือจากข้อมูลที่ได้รับจากอินเทอร์เน็ต รวมทั้งปัญหาที่สำคัญจากภัยคุกคามไซเบอร์ไม่ว่าจะเป็นไวรัส มัลแวร์ จากสถานการณ์ดังกล่าว ส่งผลให้หลายหน่วยงานที่เกี่ยวข้องต้องดำเนินการเพื่อตอบสนองต่อสถานการณ์ที่เกิดขึ้น ตามภารกิจของแต่ละหน่วยงานเพื่อสร้างความเชื่อมั่นให้เกิดขึ้น โดยในส่วนของ สพธอ. ได้ดำเนินการตามภารกิจขององค์กรไม่ว่าจะเป็น การป้องกัน ฝ้าระวังและรับมือกับภัยคุกคาม รวมทั้งแก้ไขและฟื้นฟูสถานการณ์จากปัญหาที่เกิดขึ้น ซึ่งผลการดำเนินงานของ สพธอ. ในปีงบประมาณ พ.ศ. ๒๕๖๑ มีดังนี้

Cybersecurity Missions

ในด้านการป้องกัน ฝ้าระวัง และรับมือกับภัยคุกคามไซเบอร์ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ที่จัดตั้งขึ้นและดำเนินการ เพื่อตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านการคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านการคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือ ตลอดจนแนวทางต่างๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต ซึ่งผลการดำเนินงานในปี พ.ศ. ๒๕๖๑ สพธอ. ได้สร้างความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์-มีเครือข่ายการทำงานที่เข้มแข็ง และมีการทำงานในเชิงรุก โดยการขยายระบบสนับสนุนการวิเคราะห์และป้องกันการโจมตีทางไซเบอร์ให้กับหน่วยงานภายใต้โครงการ ThaiCERT Government Monitoring System (ThaiCERT GMS) ซึ่งมีวัตถุประสงค์เพื่อฝ้าระวังการโจมตีทางไซเบอร์ให้กับหน่วยงานภาครัฐที่เข้าร่วมโครงการ ด้วย ๒ ระบบสำคัญ คือ ระบบ Government Threat Monitoring (GTM) ที่สามารถตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ และระบบ Government Website Protection (GWP) ที่สามารถ

ป้องกันภัยคุกคามที่จะเกิดขึ้นกับเว็บไซต์ โดยในส่วนของระบบ GTM มีการติดตั้งให้กับหน่วยงานภาครัฐระดับกรมจำนวน ๔๐ หน่วยงาน ซึ่งหากรวมจำนวนหน่วยงานที่ได้รับการติดตั้งระบบดังกล่าว ตั้งแต่ปีงบประมาณ พ.ศ. ๒๕๕๘ - ๒๕๖๑ จะมีจำนวนรวมทั้งสิ้น ๒๕๐ หน่วยงาน และได้ดำเนินการตรวจช่องโหว่ของเว็บไซต์ของหน่วยงานภาครัฐแล้วจำนวน ๒๔๓ เว็บไซต์ โดยรวมจำนวนเว็บไซต์ที่ผ่านการตรวจแล้วกว่า ๑,๕๐๐ เว็บไซต์ ทั้งนี้ยังได้มีการแจ้งเตือนและดำเนินการเพื่อระงับหรือป้องกันการโจมตีที่อาจส่งผลกระทบต่อระบบที่มีการฝ้าระวังภายใน ๑ ชั่วโมง หลังจากได้ผลการวิเคราะห์คิดเป็น ร้อยละ ๙๖.๙๘

นอกจากนี้ ยังได้มีการจัดตั้ง Sector based CERT ในหน่วยงานสำคัญ เช่น หน่วยงานด้านการเงิน การลงทุน การค้า โครงสร้างพื้นฐานสำคัญ เพื่อเป็นกลไกในการตอบสนองต่อภัยคุกคามไซเบอร์ ซึ่งมีพิธีลงนามบันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจการค้า อุตสาหกรรม และโครงสร้างพื้นฐานสำคัญของประเทศ โดยในปีงบประมาณ พ.ศ. ๒๕๖๑ การจัดตั้ง Sector-based CERT สำหรับกลุ่ม Financial Sector-based CERT จำนวน ๒ กลุ่ม ได้แก่ ๑) Thailand Banking Sector CERT (TB-CERT) เพื่อเสริมสร้างให้ภาคสถาบันการเงินยกระดับความพร้อมในการดูแลความ

มั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและเตรียมความพร้อมรับมือภัยคุกคามไซเบอร์ ให้สอดคล้องกับการนำเทคโนโลยีมาใช้ในการให้บริการทางการเงินอย่างกว้างขวาง เมื่อวันที่ ๒ ตุลาคม ๒๕๖๐



และ ๒) Thai Capital Market CERT (TCM-CERT) เพื่อยกระดับความพร้อมในการรับมือภัยคุกคามด้านไซเบอร์ของผู้ประกอบธุรกิจให้มีความเข้มแข็งผ่านการแลกเปลี่ยนข้อมูล การแจ้งเตือนภัย การฝึกอบรมบุคลากร และการทดสอบรับมือภัยคุกคามระหว่างกัน รวมทั้งการช่วยเหลือซึ่งกันและกันเมื่อเกิดเหตุ ซึ่งการร่วมมือกันดังกล่าวจะช่วยให้อุทธรกิจลดต้นทุนการดำเนินงานในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และช่วยเสริมสร้างความเชื่อมั่นของผู้ใช้บริการในตลาดทุน และตลาดทุนโดยรวม โดยในปี พ.ศ. ๒๕๖๑ สพธอ. กำลังอยู่ระหว่างการ

ประสานงานกับสมาคมโทรคมนาคมไทยอย่างใกล้ชิดในการดำเนินการจัดตั้ง Sector-based CERT ในกลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม ซึ่งเป็น ๑ ใน ๖ กลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ

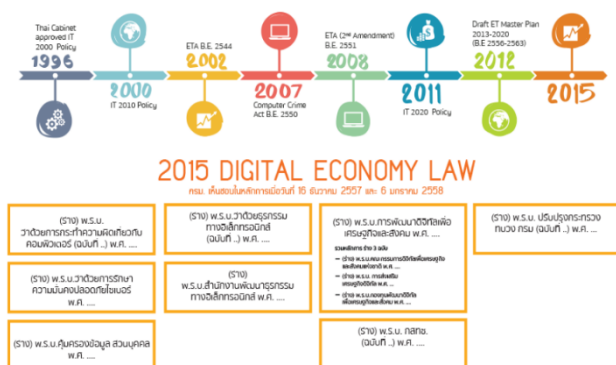
งานในส่วนของการบริการตรวจพยานหลักฐานดิจิทัล โดยศูนย์ดิจิทัลพอเรนสิคส์ ตรวจพิสูจน์พยานหลักฐานดิจิทัลไปแล้ว ๒๔ กรณี ปริมาณข้อมูล ๒๖ เทราไบต์ และได้มีการปรับปรุงเครื่องมือตรวจพิสูจน์พยานหลักฐานดิจิทัลให้รองรับอุปกรณ์โทรศัพท์มือถือและพยานหลักฐานดิจิทัลประเภทภาพ เสียง และวีดีโออีกด้วย



Infrastructure/Soft Infrastructure

ในด้านการสร้างมาตรการป้องกันเพื่อสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ สพธอ. ได้ดำเนินการจัดทำและผลักดันร่างกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ของประเทศ ได้แก่ ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นกลไกสำคัญในการกำหนดแนวทางและมาตรการต่างๆ ที่เกี่ยวข้อง อย่างเป็นรูปธรรม เพื่อการรับมือกับภัยคุกคามทางไซเบอร์ที่มีจำนวนที่เพิ่มสูงขึ้นและทวีความรุนแรงขึ้น

นอกจากนี้ยังมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และร่างพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งเป็นกฎหมายที่จะมีส่วนช่วยสร้างความเชื่อมั่นและอำนวยความสะดวกให้กับภาคธุรกิจและภาคประชาชน ซึ่งพระราชบัญญัติและร่างพระราชบัญญัตินี้ดังกล่าวข้างต้น เป็นเพียงส่วนหนึ่งของชุดร่างกฎหมายเพื่อการส่งเสริมเศรษฐกิจและสังคม หรือเรียกสั้นๆ ว่า “ชุดกฎหมายเศรษฐกิจดิจิทัล” (Digital Economy)



โดยชุดกฎหมายเศรษฐกิจดิจิทัล จำนวน ๘ ฉบับ ที่คณะรัฐมนตรีได้อนุมัติหลักการไปแล้วนั้น เป็นการผ่านการพิจารณาในระดับนโยบายว่า ในหลักการประเทศไทยควรมีกฎหมายในเรื่องเหล่านี้ โดยปัจจุบันมีพระราชบัญญัติที่ผ่านการพิจารณาตามลำดับและได้ประกาศในราชกิจจานุเบกษาแล้วจำนวน ๔ ฉบับ ซึ่งสามารถติดตามสถานะของชุดกฎหมายเศรษฐกิจดิจิทัลรวมทั้งกฎหมายเทคโนโลยีสารสนเทศ คำอธิบายกฎหมายและประเด็นร้อน (Hot Issue) ที่เกี่ยวข้องได้จากศูนย์กฎหมาย ICT Law Center ผ่านเว็บไซต์ <https://ictlawcenter.etcha.or.th/>

และอีกหนึ่งกลไกสำคัญที่จะช่วยสร้างความเชื่อมั่นให้เกิดขึ้นได้ในวงกว้าง หากผู้ใช้งานสามารถยืนยันตัวตนและได้รับการดูแลรักษาความถูกต้องของข้อมูลจากการรับบริการต่างๆ ของภาครัฐและภาคเอกชน ในปีงบประมาณ พ.ศ. ๒๕๖๑ สพอ. ได้ดำเนินการพัฒนาระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล ซึ่งเป็นการให้บริการเพื่อใช้ยืนยันตัวตนทางดิจิทัลตามมาตรฐาน Open ID Connect Protocol สำหรับให้บริการแก่หน่วยงานทั่วไป โดยในปีงบประมาณ พ.ศ. ๒๕๖๑ ได้มีการลงนามบันทึกข้อตกลงความร่วมมือกับ กองทุนเงินให้กู้ยืมเพื่อการศึกษา (กยศ.) และมหาวิทยาลัยศรีนครินทรวิโรฒ (มศว.) ในการเชื่อมโยงระบบการยืนยันตัวตนและแลกเปลี่ยนข้อมูลของผู้กู้ยืมเงินกองทุน เพื่อประโยชน์ในการนำข้อมูลมาใช้กู้ยืมและบริหารจัดการหนี้ โดยร่วมกันพัฒนา ทดสอบ และนำร่องการใช้งานระบบพิสูจน์และยืนยันตัวตนทางดิจิทัล เพื่ออำนวยความสะดวกแก่

นักศึกษาและบุคลากรของมหาวิทยาลัยในการเข้าถึงบริการด้านการกู้ยืมของ กยศ. เมื่อวันที่ ๒๔ กรกฎาคม ๒๕๖๑ และเตรียมขยายผลการใช้งานระบบในปีงบประมาณ พ.ศ. ๒๕๖๒ ต่อไป



รวมทั้งได้จัดทำข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ได้แก่ ๑) ประกาศข้อเสนอแนะมาตรฐานฯ ว่าด้วยการทำธุรกรรมแบบพบเห็นลูกค้าต่อหน้าสำหรับธนาคาร ประกาศเมื่อวันที่ ๓๐ มีนาคม ๒๕๖๑ และ ๒) ประกาศข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทย จำนวน ๓ ฉบับ ประกอบไปด้วย ภาพรวมและอภิธานศัพท์ การลงทะเบียนและพิสูจน์ตัวตน และการยืนยันตัวตน ซึ่งได้ประกาศใช้เมื่อวันที่ ๒๗ กันยายน ๒๕๖๑ ที่ผ่านมา โดยสามารถศึกษาข้อเสนอแนะมาตรฐานฯ ที่เกี่ยวข้องกับการอำนวยความสะดวกทางการค้าและธุรกรรมทางอิเล็กทรอนิกส์เพิ่มเติมได้ที่เว็บไซต์ <https://standard.etcha.or.th/>



Policy

การสร้างมาตรการป้องกันเชิงนโยบายถือได้ว่าเป็นอีกกลไกหนึ่งที่สำคัญเพื่อสนับสนุนให้เกิดการดำเนินงานที่เป็นไปในทิศทางเดียวกันในระยะยาว โดย สทอ. ได้รับมอบหมายจากคณะกรรมการเตรียมการไซเบอร์ฯ ในการเป็นหน่วยประสานงานกลางเป็นการชั่วคราวระหว่างจัดตั้ง Cybersecurity Agency (CSA) เพื่อรับมือภัยคุกคามทางไซเบอร์ และทำงานร่วมกับหน่วยงานที่เกี่ยวข้อง ในการลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์



โดยทำหน้าที่เป็นหน่วยประสานงานกลาง และหน่วยงานเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความปลอดภัยมั่นคงไซเบอร์ของชาติอยู่ในระดับมาตรฐานสากล ซึ่งสืบเนื่องมาจากการประชุมคณะเตรียมการด้านการรักษาความปลอดภัยมั่นคงไซเบอร์แห่งชาติ ครั้งที่ ๑/๒๕๖๑ โดยมี พลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี เป็นประธานการประชุม ซึ่งมีประเด็นสำคัญในการประชุมดังกล่าว ได้แก่

- ๑) กรอบนโยบายและแผนระดับชาติ เพื่อปกป้อง รับมือ ป้องกัน และลดความเสี่ยง ให้มีทิศทางเดียวกัน
- ๒) แนวทางการกำหนดโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ของประเทศ และแนวปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางความมั่นคงปลอดภัยไซเบอร์ (Standard Operating Procedure: SOP) โดยกลุ่มโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ จำนวน ๖ กลุ่ม ได้แก่ กลุ่มความมั่นคงและบริการภาครัฐ กลุ่มการเงิน กลุ่มเทคโนโลยีสารสนเทศและโทรคมนาคม กลุ่มการขนส่งและโลจิสติกส์ กลุ่มพลังงานและสาธารณูปโภค และกลุ่มสาธารณสุข
- ๓) แนวทางการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระยะเร่งด่วน
- ๔) แนวทางการจัดตั้ง Cybersecurity Agency (CSA) ทำหน้าที่เป็นหน่วยประสานงานกลางและหน่วยงานเผชิญเหตุด้านความมั่นคง ปลอดภัยไซเบอร์ชั่วคราว เพื่อให้ความปลอดภัยมั่นคงไซเบอร์ของชาติอยู่ในระดับมาตรฐานสากล

Manpower

นอกจากนี้เพื่อเป็นการเตรียมความพร้อมเพื่อรับมือกับปัญหาด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นได้กับภาคส่วนสำคัญที่เป็นโครงสร้างพื้นฐานของประเทศ รวมไปถึงหน่วยงานภาครัฐที่ทำหน้าที่ให้บริการแก่ประชาชน จึงได้มีการวางแผนและพัฒนากำลังคนดิจิทัล โดย สทอ. ได้ดำเนินการพัฒนาศักยภาพบุคลากรทั้งภายในและต่างประเทศในด้านความมั่นคงปลอดภัยไซเบอร์ภายใต้โครงการ Cybersecurity Missions ในปีงบประมาณ พ.ศ. ๒๕๖๑ รวม ๓๑๒ คน ผ่านการจัดกิจกรรมเพื่อเพิ่มทักษะด้านการป้องกัน รับมือ และแก้ไขปัญหาภัยคุกคาม เช่น การจัดหลักสูตร IT Security

Management หลักสูตรอบรมด้านดิจิทัลฟอเรนสิคส์ การฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ (Cyber Drill) และ Table Top Exercise เป็นต้น นอกจากนี้ ในปีงบประมาณ พ.ศ. ๒๕๖๑ ยังได้ประกาศความร่วมมือกับ ๖ มหาวิทยาลัย ได้แก่ มหาวิทยาลัยมหิดล มหาวิทยาลัยธรรมศาสตร์ มหาวิทยาลัยศิลปากร มหาวิทยาลัยหอการค้าไทย มหาวิทยาลัยรังสิต และ มหาวิทยาลัยเกษตรศาสตร์ ในการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ให้เป็นไปตามแผนพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

และยังได้รับการคัดเลือกให้เป็นเจ้าภาพหลักในการจัดตั้งศูนย์ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ หรือ ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) ในประเทศไทย ได้เปิดตัวอย่างเป็นทางการเมื่อวันที่ ๑๔ กันยายน ๒๕๖๑ โดยมี ดร. พิเชฐ ดุรงคเวโรจน์ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานในพิธีเปิด ซึ่งศูนย์ AJCCBC มีกำหนดจัดการฝึกอบรมสำหรับข้าราชการและเจ้าหน้าที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของอาเซียนครั้งแรกในวันที่ ๒๔-๒๘ กันยายน ๒๕๖๑ สำหรับหลักสูตรที่

ใช้ในการฝึกอบรมประกอบด้วย ๓ หลักสูตร คือ ๑) หลักสูตร CYDER (Cyber Defense Exercise with Recurrence) ที่เน้นการรับมือกับภัยคุกคามทางไซเบอร์ ๒) หลักสูตร Forensics เป็นหลักสูตรที่เกี่ยวข้องกับการตรวจพิสูจน์พยานหลักฐานดิจิทัลจากการโจมตีทางไซเบอร์ และ ๓) หลักสูตร Malware Analysis ที่จะเป็นการวิเคราะห์มัลแวร์ประเภทต่าง ๆ ตามเทรนด์ของภัยคุกคามทางไซเบอร์ ซึ่งถือได้ว่าเป็นโอกาสที่จะได้สร้างบุคลากรด้านความมั่นคงปลอดภัยในภูมิภาคเพื่อการประสานความร่วมมือที่ต่อไปในอนาคตอีกด้วย



และไม่เพียงแต่กำลังคนด้านความมั่นคงปลอดภัยไซเบอร์เท่านั้น สฟทอ. ยังได้พัฒนากำลังคนในด้านที่เกี่ยวข้องควบคู่กันไปทั้งระบบที่มีความเกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์โดยมุ่งเน้นไปที่การรู้เท่าทัน การใช้งานอย่างมั่นคงปลอดภัย และการเพิ่มพูนความรู้ความเข้าใจ ตลอดจนใช้เป็นช่องทางหารายได้ ตัวอย่างเช่น การบรรยายและเผยแพร่ความรู้ด้านกฎหมายดิจิทัลให้กับหน่วยงานและประชาชนทั่วไปจำนวน ๑,๒๒๗ คน ซึ่งองค์ความรู้ด้านกฎหมายที่ทำการเผยแพร่ นั้นถือได้ว่าเป็นประโยชน์ในวงกว้าง ไม่ว่าจะเป็น การบรรยายหัวข้อ "การรู้เท่าทันสื่อ และ พ.ร.บ.คอมพิวเตอร์"



"กฎหมายเทคโนโลยีสารสนเทศ" "วิธีใช้งานลายมือชื่ออิเล็กทรอนิกส์ (Digital Signature)" เป็นต้น รวมทั้งการเพิ่มพูนองค์ความรู้ให้กับผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) เพื่อการดำเนินธุรกิจอย่างมั่นคงปลอดภัย สร้างความน่าเชื่อถือเชื่อมั่นให้กับผู้บริโภค โดยในปีงบประมาณ พ.ศ. ๒๕๖๑ ได้ดำเนินการพัฒนาศักยภาพผู้ประกอบการกว่า ๑,๐๐๐ ราย ภายใต้หลักสูตรสำคัญเพื่อการพาณิชย์อิเล็กทรอนิกส์ เช่น นวัตกรรมการเงินสำหรับ SMEs ในยุค Thailand 4.0 การ



สร้างธุรกิจในยุคเศรษฐกิจดิจิทัล และไปกำกับภาษีอิเล็กทรอนิกส์ เป็นต้น นอกจากนี้ยังได้ดำเนินการคัดเลือกผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์เข้าสู่ e-Directory (Thai e-Market.com) ซึ่งเป็นศูนย์กลางและเป็นแหล่งรวมสินค้าจากผู้ประกอบการไทยทั่วประเทศที่ผ่านการคัดกรองคุณภาพและมาตรฐานร้านค้าจากผู้ดูแลระบบของ สฟทอ. ผู้บริโภคจึงสามารถมั่นใจได้ว่าทั้งสามารถทำธุรกรรมได้อย่างปลอดภัย โดยปัจจุบันมีผู้ประกอบการอยู่ภายใต้ e-Directory นี้กว่า ๘,๐๐๐ รายด้วยกัน



Central Coordinator

ไม่เพียงแต่การดำเนินงานภายใต้ภารกิจหลักเท่านั้น สฟธอ. ยังได้ขยายความร่วมมือไปยังหน่วยงานต่างๆ ทั้งในประเทศและต่างประเทศ ไม่ว่าจะเป็นหน่วยงานสำคัญสาย Regulators และสายเศรษฐกิจ รวมทั้งโครงสร้างพื้นฐานสำคัญของประเทศ ได้แก่ กลุ่ม Finance กลุ่มพลังงาน ไฟฟ้า โทรคมนาคม และ ISP เพื่อร่วมกันผลักดันให้เกิดความร่วมมือในการแก้ไขปัญหาภัยคุกคามไซเบอร์ที่อาจกระทบต่อความมั่นคงและเสถียรภาพของประเทศ และสร้างเครือข่ายความร่วมมือกับหน่วยงานต่างประเทศ เช่น JPCERT/CC (Japan Computer Emergency Response Team Coordination Center), APWG (Anti-Phishing Working Group), LaoCERT, Computer Crime Institute (Dixie State University), SANS Institute, EC-Council, Ministry of Internal Affairs and Communications (Japan), Korea Internet Security Agency (KISA), Cybersecurity Malaysia เป็นต้น

เมื่อการดำเนินงานด้านการป้องกัน เฝ้าระวัง รับมือ และพัฒนาศักยภาพบุคลากรเพื่อเตรียมความพร้อมให้กับประเทศแล้ว ในด้านการแก้ไขปัญหาที่เกิดขึ้น สฟธอ. ยังได้ดำเนินการจัดตั้งศูนย์รับเรื่องร้องเรียนออนไลน์ (1212 Online Complaint Center) ซึ่งถือเป็นศูนย์กลางในการรับเรื่องร้องเรียนที่เกี่ยวข้องกับปัญหาอันเกิดจากการทำธุรกรรมออนไลน์ และให้คำแนะนำเบื้องต้นเกี่ยวกับแก้ไขปัญหาที่เกิดขึ้นหรือการประสานไปยังหน่วยงานที่เกี่ยวข้องตามที่มีการลงนามใน MOU ร่วมกัน คือ สำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) สำนักงานคณะกรรมการอาหารและยา (อย.) กรมพัฒนาธุรกิจการค้า และกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับ



อาชญากรรมทางเทคโนโลยี (บก.ปอท.) อย่างต่อเนื่อง มีสถิติการใช้บริการฯ ตั้งแต่จัดตั้งศูนย์ฯ จนถึงปัจจุบันมีจำนวนเรื่องร้องเรียนทั้งสิ้น ๕๔,๓๗๑ เรื่อง โดยปัญหาที่พบจากการรับเรื่องร้องเรียนพบว่าเป็นเรื่องของปัญหาจากการซื้อขายออนไลน์ และปัญหาเว็บไซต์ผิดปกติ ตามลำดับ ซึ่งถือได้ว่าศูนย์รับเรื่องร้องเรียนออนไลน์เป็นที่พึ่งของผู้บริโภคและผู้ประกอบการในการแก้ไขปัญหาที่เกิดขึ้นจากการซื้อขายสินค้าออนไลน์ และช่วยสร้างความเชื่อมั่นให้เกิดขึ้นอีกด้วย

Awareness

อีกด้านหนึ่งของการป้องกันและแก้ไขปัญหาจากการใช้อินเทอร์เน็ต จึงเป็นการสร้างการตระหนักรู้ ความเข้าใจเกี่ยวกับการใช้เทคโนโลยีสารสนเทศ เพื่อให้เกิดการใช้อินเทอร์เน็ตอย่างมั่นคงปลอดภัย โดยเริ่มจากกลุ่มเป้าหมายสำคัญที่ได้จากผลการสำรวจ ซึ่งพบว่ากลุ่มเด็ก เยาวชน และผู้สูงอายุ ถือว่าเป็นกลุ่มที่มีการใช้อินเทอร์เน็ตในลำดับต้น ๆ จึงทำให้เผชิญกับความเสี่ยงและอันตรายจากการใช้งานอินเทอร์เน็ตสูง สฟธอ. จึงดำเนินการจัดทำหลักสูตรและสื่อเผยแพร่ความรู้ โดยมุ่งเน้นที่กลุ่มเด็ก เยาวชน และผู้สูงอายุ เพื่อให้มีความตระหนักรู้ ความเข้าใจเกี่ยวกับการใช้เทคโนโลยีสารสนเทศ



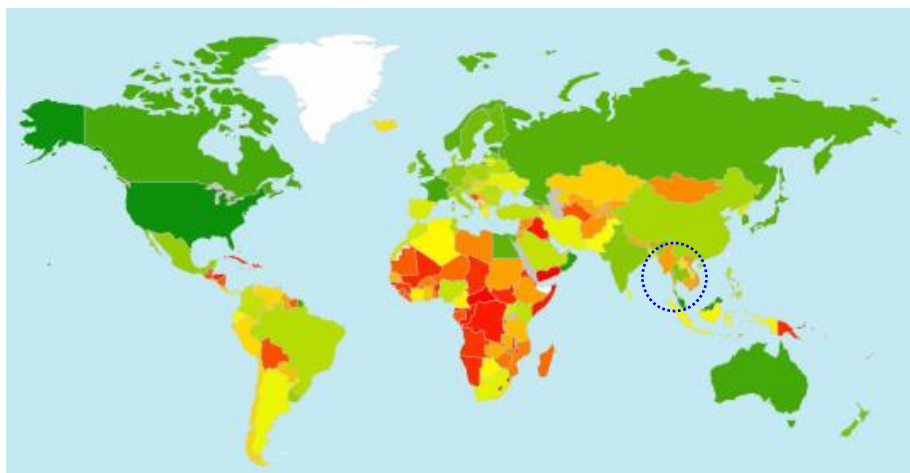
ซึ่งในปีงบประมาณ พ.ศ. ๒๕๖๑ ได้ดำเนินการจัดทำหลักสูตรจำนวน ๒ หลักสูตรสำหรับเด็กเยาวชนและผู้สูงอายุ รวมทั้งสื่ออินโฟกราฟิกจำนวน ๘ เรื่อง และหนังสือประกอบการจัดกิจกรรมจำนวน ๑ เล่ม นอกจากนี้ ยังได้จัดกิจกรรมอบรม ให้กลุ่มเป้าหมายทั่วประเทศจำนวน ๔,๑๑๖ คน ซึ่งพบว่าผู้เข้าอบรมมีความพึงพอใจต่อกิจกรรมคิดเป็น ร้อยละ ๗๒.๑๘ และ ผู้เข้าร่วมอบรมมีความรู้ความเข้าใจเพิ่มขึ้นคิดเป็น ร้อยละ ๙๓.๕๖ โดยตั้งเป้าหมายที่จะดำเนินการอย่างต่อเนื่องในปีงบประมาณ พ.ศ. ๒๕๖๒ ต่อไป



นอกจากกลุ่มดังกล่าวข้างต้นแล้ว สฟธอ. ยังได้ให้ความสำคัญในการสร้างความตระหนักรู้ต่อสาธารณชนด้วยการจัดทำข้อมูลด้านความมั่นคงปลอดภัยอย่างต่อเนื่องทั้งในรูปแบบของหนังสือคู่มือ และอินโฟกราฟิกเพื่อเผยแพร่และสร้างความตระหนักรู้ต่อสาธารณะในวงกว้าง ได้แก่ หนังสือ Cyber Threat 2011-2017 และอินโฟกราฟิก เรื่องต่างๆ เช่น Phishing Awareness, Email Scam Awareness, Malicious Code Awareness, Security tips while travelling, How to protect from WannaCry เป็นต้น ซึ่งสามารถดาวน์โหลดได้จาก <https://www.etda.or.th/documents-for-download.html> ซึ่งชุดข้อมูลดังกล่าวทำให้ทราบถึงวิธีการป้องกันภัยคุกคามไซเบอร์ ที่สามารถนำมาปฏิบัติก่อนที่จะตกเป็นเหยื่อภัยคุกคามไซเบอร์ต่างๆ เพื่อให้เกิดการใช้งานเทคโนโลยีและก้าวไปในโลกที่เปลี่ยนแปลงได้อย่างมั่นใจอีกด้วย

Trust

จะเห็นได้ว่าการดำเนินงานตามภารกิจของ สฟธอ. นั้น เป็นการดำเนินงานที่แสดงให้เห็นถึงการยกระดับด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ทั้งด้านมาตรการกฎหมาย (Legal Measures) มาตรการด้านเทคนิค (Technical Measures) ด้านการพัฒนาบุคลากร (Capacity Building) มาตรการเกี่ยวกับองค์กร (Organization Measures) และความร่วมมือ (Cooperation) ส่งผลให้การจัดลำดับ Global Cybersecurity Index โดย International Telecommunication Union (ITU) ในปี พ.ศ. ๒๕๖๐ ซึ่งเป็นประเมินความพร้อมด้าน Cybersecurity ของประเทศต่าง ๆ ทั่วโลก ซึ่งประเทศไทยอยู่อันดับที่ ๒๒ จากทั้งหมด ๑๖๕ อันดับ (๑๙๓ ประเทศ) จากภาพจะเห็นได้ว่าประเทศไทยมีระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับสูง (สีเขียว)



https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

หากการดำเนินงานดังกล่าวข้างต้นของ สพอ. ยังคงเป็นไปอย่างต่อเนื่องก็จะสามารถสร้างความเชื่อมั่นให้เกิดขึ้นในวงกว้าง ไม่ว่าจะเป็นการเข้าถึงและใช้งานอินเทอร์เน็ตเพื่อกิจกรรมต่างๆ ในชีวิตประจำวันได้อย่างมั่นคงปลอดภัย โดยเฉพาะอย่างยิ่งการทำธุรกรรมทางอิเล็กทรอนิกส์ รวมถึงการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) ซึ่ง สพอ. ได้ดำเนินการเพื่อสนับสนุนการพาณิชย์อิเล็กทรอนิกส์อย่างต่อเนื่อง ด้วยการจัดเก็บข้อมูลสถิติสำคัญเพื่อใช้เป็นประกอบการวางแผนและกำหนดแนวทาง และเป็นแหล่งข้อมูลสำหรับที่สะท้อนถึงสภาพภาพของประเทศไทยในการจัดอันดับในเวทีระหว่างประเทศด้วย ซึ่งจากผลการสำรวจที่ผ่านมาพบว่า มูลค่าพาณิชย์อิเล็กทรอนิกส์ของประเทศไทยในระหว่างปี ๒๕๕๗-๒๕๖๑ มีอัตราการเติบโตสูงถึง ร้อยละ ๓๘.๓๑ โดยเฉพาะอย่างยิ่งการพาณิชย์อิเล็กทรอนิกส์ในส่วนของ B2C หรือ Business to Customer ซึ่งมีอัตราการเติบโตเพิ่มสูงขึ้นทุกปีจากผลการสำรวจพบว่าประเทศไทยยังคงเป็นอันดับ ๑ ในภูมิภาคอาเซียนอีกด้วย

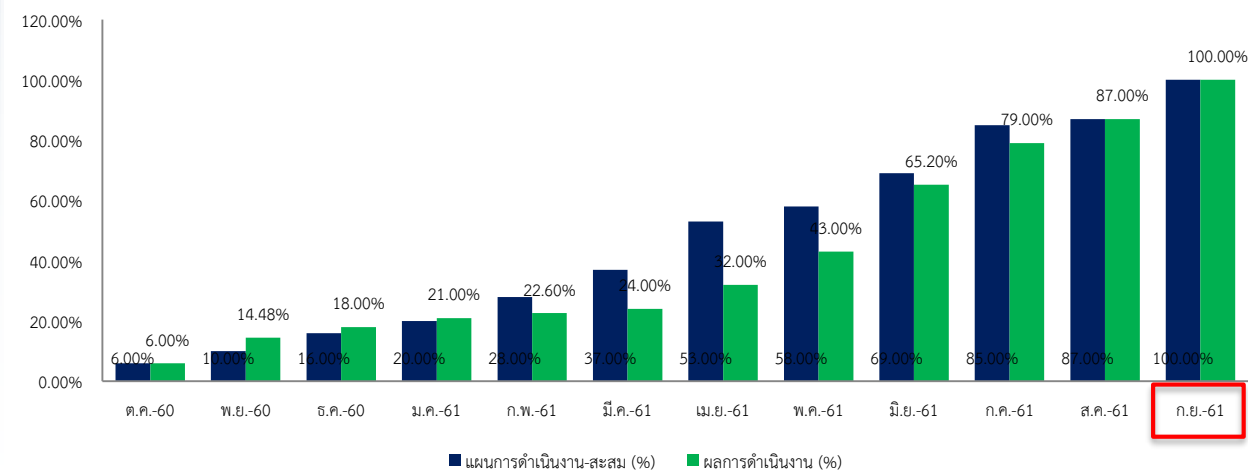


สรุปแผน/ผลการดำเนินงานตามตัวชี้วัดโครงการ ประจำปีงบประมาณ พ.ศ. 2561

หมายเหตุ : ผ่านความเห็นชอบจากคณะกรรมการบริหาร สพรอ. ในการประชุมครั้งที่ 11/2561 (วาระที่ 3 ครั้งที่ 2) เมื่อวันที่ 3 ตุลาคม 2561

สรุปแผน/ผลการดำเนินงานตามตัวชี้วัดโครงการ Cybersecurity Missions

ตัวชี้วัดโครงการ ปีงบประมาณ พ.ศ. 2561	แผน ปี61	ผล ปี61	ผล ปี60	ผล ปี59
1. จำนวนหน่วยงานที่มีระบบป้องกัน/เฝ้าระวังภัยคุกคามทางเทคโนโลยีสารสนเทศ	40 หน่วยงาน	40 หน่วยงาน	36 หน่วยงาน	84 หน่วยงาน
2. จำนวนเว็บไซต์ที่มีระบบป้องกัน/เฝ้าระวังภัยคุกคามทางเทคโนโลยีสารสนเทศ	240 เว็บไซต์	243 เว็บไซต์	365 เว็บไซต์	339 เว็บไซต์
3. ระบบตรวจสอบและป้องกันภัยคุกคาม ที่แฝงเข้ามาผ่านอีเมลของหน่วยงานของรัฐ (GMP)	1 ระบบ	1 ระบบ	-	-
4. ระบบโดเมน (DNS) ของหน่วยงานรัฐ เพื่อตรวจจับการเชื่อมต่อของมัลแวร์จากระบบภายในหน่วยงานรัฐ (GDNS)	1 ระบบ	1 ระบบ	-	-
5. ระบบบริการตรวจพยานหลักฐานดิจิทัลประเภทภาพ เสียง และวิดีโอ	1 ระบบ	1 ระบบ	-	-
6. อัปเดตเครื่องมือตรวจพิสูจน์พยานหลักฐานดิจิทัลให้รองรับอุปกรณ์โทรศัพท์มือถือ และพยานหลักฐานดิจิทัลประเภทภาพ เสียง และวิดีโอตั้งแต่ปีงบประมาณ 2558 หรือใหม่กว่า	ร้อยละ 80	ร้อยละ 100	-	-
7. จำนวนชุดข้อมูล Data set ที่สามารถเปิดเผยให้ประชาชนและภาคธุรกิจสามารถนำไปใช้ประโยชน์	1 ชุดข้อมูล	1 ชุดข้อมูล	1 ชุดข้อมูล	-
8. มาตรฐานการให้บริการที่สอดคล้องกับมาตรฐานสากลที่สามารถรักษาสถานภาพไว้ (ISO 17025 หรือ ISO 27001)	1 ใบรับรอง	1 ใบรับรอง	1 ใบรับรอง	-
9. ผู้เข้ารับการอบรมเชิงลึก/กิจกรรม เพื่อยกระดับทักษะด้านการทำธุรกรรมออนไลน์/ความมั่นคงปลอดภัยทางไซเบอร์	300 คน	312 คน	445 คน	750 คน
10. การแจ้งเตือนและดำเนินการเพื่อลดความเสี่ยงจากการโจมตีที่อาจส่งผลกระทบต่อระบบที่มีการเฝ้าระวังในโครงการ	ร้อยละ 90	ร้อยละ 96.8	ต่ำกว่า 24 ชม.	ต่ำกว่า 24 ชม.
11. ระบบ Secure Digital Forensic Archive (SDFA) (ตัวชี้วัดเพิ่มเติมจากข้อเสนอโครงการฯ)	1 ระบบ	1 ระบบ	-	-



ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

PRIVACY SECURITY

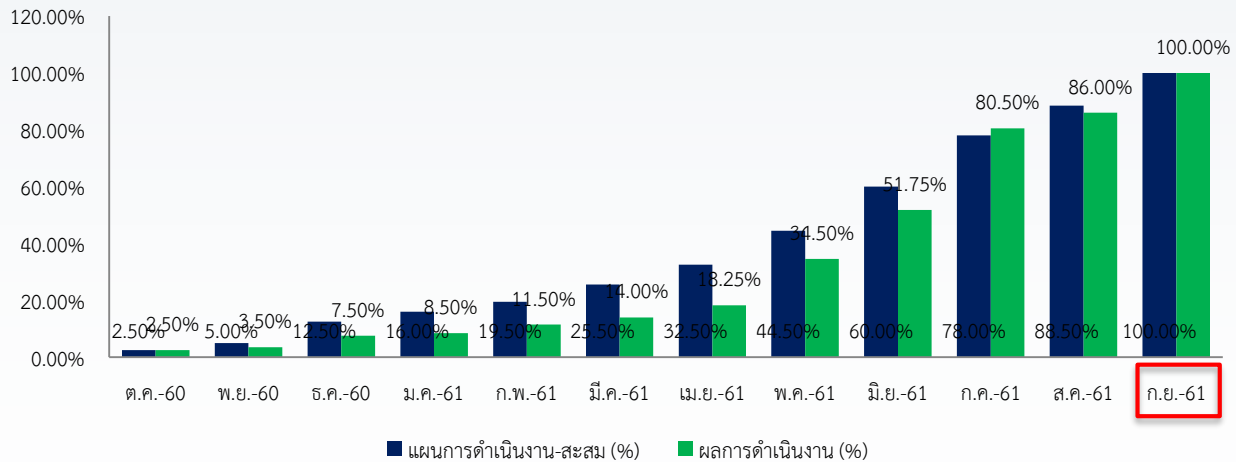
ผลการดำเนินงานโครงการ ปี 2561

แผน: 100%
ผล: 100%

(ข้อมูล ณ เดือนกันยายน 2561)

ตัวชี้วัดโครงการ ปีงบประมาณ พ.ศ. 2561	แผน ปี61	ผล ปี61	ผล ปี60	ผล ปี59
1. จำนวนชุดข้อมูล data Set ที่สามารถเปิดเผยให้ประชาชนและภาคธุรกิจสามารถนำไปใช้ประโยชน์	3 ชุดข้อมูล	3 ชุดข้อมูล	3 ชุดข้อมูล*	4 ชุดข้อมูล*
2. จำนวนรายงานผลการสำรวจเชิงลึกด้านการทำธุรกรรมทางอิเล็กทรอนิกส์	2 เรื่อง	2 เรื่อง	3 เรื่อง *	4 เรื่อง*
3. จำนวนผู้เข้าร่วมโครงการในการให้ข้อมูลและระดมความคิดเห็น	300 คน	300 คน	554 คน	-
4. จำนวนกิจกรรมที่ส่งเสริมด้านการทำธุรกรรมออนไลน์/ความมั่นคงปลอดภัยทางไซเบอร์	4 ครั้ง	4 ครั้ง	-	-

- * **หมายเหตุ :** - การสำรวจสถิติการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทย (e-Transactions) /ดำเนินการในปี 2559
 - การสำรวจสถิติ Cybersecurity Survey /ดำเนินการในปี 2559
 - การสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตประเทศไทย (Internet User Profile) /ดำเนินการในปี 2559-2560
 - การสำรวจมูลค่าพาณิชย์อิเล็กทรอนิกส์ในประเทศไทย (e-Commerce Survey) /ดำเนินการในปี 2558-2560
 - การสำรวจสถานภาพตัวชี้วัดกลุ่ม ICT-Enabled Services (Pilot Project) /ดำเนินการในปี 2560

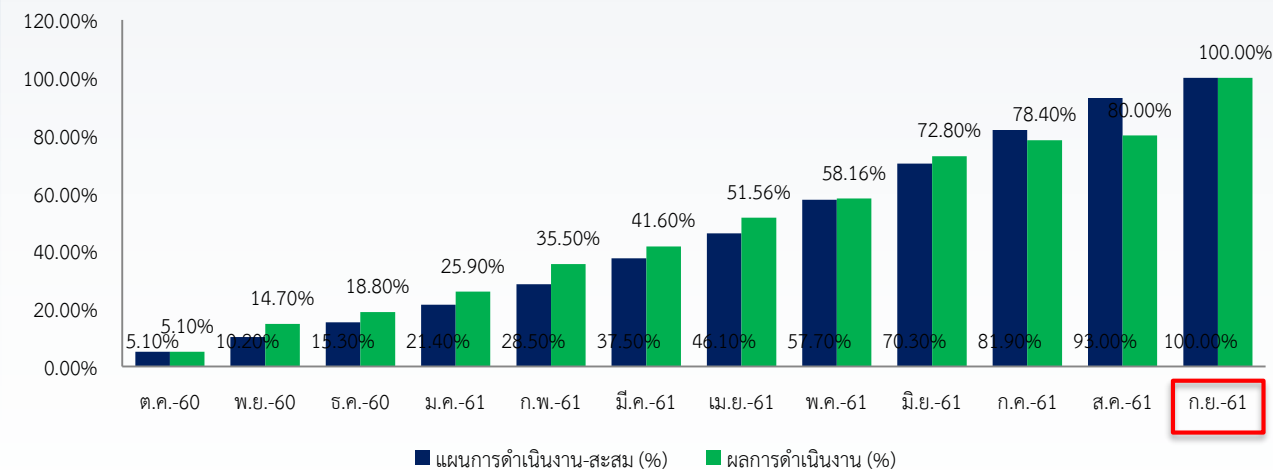


ผลการดำเนินงานโครงการ ปี 2561

แผน: 100%
 ผล: 100%
 (ข้อมูล ณ เดือนกันยายน 2561)

หมายเหตุ: แผนการดำเนินงานโครงการจะมีการทบทวน ปีละ 1 ครั้ง (ช่วงหลังไตรมาสที่ 2)

ตัวชี้วัดโครงการ ปีงบประมาณ พ.ศ. 2561	แผน ปี61	ผล ปี61	ผล ปี60	ผล ปี59
1. จำนวนผู้เข้ารับการอบรมเชิงลึก/กิจกรรม เพื่อยกระดับทักษะด้านการทำธุรกรรมออนไลน์/ความมั่นคงปลอดภัยทางไซเบอร์	600 คน	1,075 คน	1,695 คน	893 คน
2. ข้อมูลกฎหมายและที่เกี่ยวข้องที่สามารถใช้เป็นแหล่งอ้างอิง/สืบค้นข้อมูลในแหล่งเผยแพร่ของ ICT Law Center	ต่อเนื่อง	ผู้ใช้งาน (ซ้ำ IP) 501,462 ครั้ง	ผู้ใช้งาน (ซ้ำ IP) 448,437 ครั้ง	ผู้ใช้งาน(ซ้ำ IP) 248,944 ครั้ง
3. มีข้อมูล/คำอธิบายกฎหมายด้านเทคโนโลยีสารสนเทศและเศรษฐกิจดิจิทัลเผยแพร่ในรูปแบบต่างๆ	1 เรื่อง	1 เรื่อง	1 เรื่อง	4 เรื่อง
4. จำนวน (ร่าง) นโยบาย/แผน/กฎหมาย/กฎระเบียบ/มาตรฐาน ที่เอื้อต่อการใช้ประโยชน์ด้านเศรษฐกิจดิจิทัล	1 เรื่อง	1 เรื่อง	1 เรื่อง Online Consumer Protection)	1 เรื่อง (Data Privacy)
5. ร้อยละความพึงพอใจของผู้รับบริการ	ร้อยละ 80	ร้อยละ 87.53	ร้อยละ 86.24	ร้อยละ 97.11



ผลการดำเนินงานโครงการ ปี 2561

 **แผน: 100%**
ผล: 100%
 (ข้อมูล ณ เดือนกันยายน 2561)

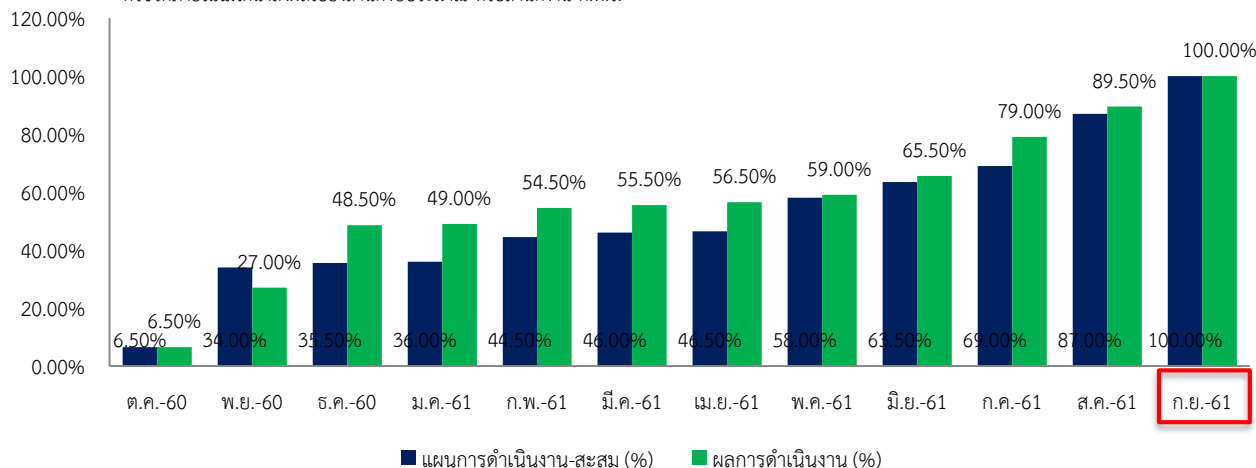
หมายเหตุ: แผนการดำเนินงานโครงการจะมีการทบทวน ปีละ 1 ครั้ง (ช่วงหลังไตรมาสที่ 2)

สรุปแผน/ผลการดำเนินงานตามตัวชี้วัดโครงการ Thailand e-Commerce Sustainability

ตัวชี้วัดโครงการ ปีงบประมาณ พ.ศ. 2561	แผน ปี61	ผล ปี61	ผล ปี60	ผล ปี59
1. การเพิ่มขึ้นของยอดขายของผู้ประกอบการใน e-Directory	ร้อยละ 30	ร้อยละ 33.33	ร้อยละ 30.44	-
2. กระตุ้นการทำพาณิชย์อิเล็กทรอนิกส์และส่งเสริมความรู้ พัฒนาทักษะ/บ่มเพาะผู้ประกอบการอีคอมเมิร์ซไทย (SMEs Go Online)				
- จำนวนผู้เข้ารับการอบรมเชิงลึก/กิจกรรม เพื่อยกระดับทักษะด้านการทำธุรกรรมออนไลน์ฯ	5,000 ราย	5,862 ราย	272 ราย	220 ราย
- กิจกรรมกระตุ้นการทำพาณิชย์อิเล็กทรอนิกส์ (Thailand e-Commerce Week)	1 ครั้ง	1 ครั้ง	1 ครั้ง	-
3. มีการจัดงาน Thailand Online Mega Sales โดยที่	1 ครั้ง	1 ครั้ง	1 ครั้ง	1 ครั้ง*
- มีจำนวนผู้ร่วมงาน (ไม่ต่ำกว่า)	100,000 ราย	145,022 ราย	965,816 ราย	451,863 ราย*
- มีมูลค่าซื้อขายทางออนไลน์เกิดขึ้นจากงานนี้ (ไม่ต่ำกว่า)	50 ล้านบาท	22 ล้านบาท**	97.8 ล้านบาท	350 ล้านบาท*
4. จำนวน Payment Partner ด้าน e-Payment เข้าร่วมโครงการฯ (สนับสนุน/ส่งเสริมสิทธิประโยชน์แก่ ผปก.)	2 หน่วยงาน	4 หน่วยงาน	5 หน่วยงาน	-
5. ร้อยละของผู้ประกอบการใน e-Directory ที่เชื่อมต่อกับ Payment Partner (ตามตัวชี้วัดที่ 4)	ร้อยละ 30	ร้อยละ 69	ร้อยละ 36.59	-
6. ระบบ call center (1212) (รวม Customer relationship management: CRM)	1 ระบบ	1 ระบบ	1 ระบบ	-
7. ร้อยละความพึงพอใจของผู้รับบริการ (OCC) –สรุปผลปลายปีงบประมาณฯ-	ร้อยละ 80	ร้อยละ 87	ร้อยละ 83	ร้อยละ 81.27

หมายเหตุ: * เป็นการดำเนินงานกิจกรรมภายใต้โครงการ SMEs GO ONLINE ซื่อขายมันใจ มีปัญหาเมื่อไร เราดูแล (Flagship)

** ตัวชี้วัดภายในไม่ได้นำเสนอผลไปยังสำนักงบประมาณ หรือสำนักงาน ก.พ.ร.








ผลการดำเนินงานโครงการ ปี 2561

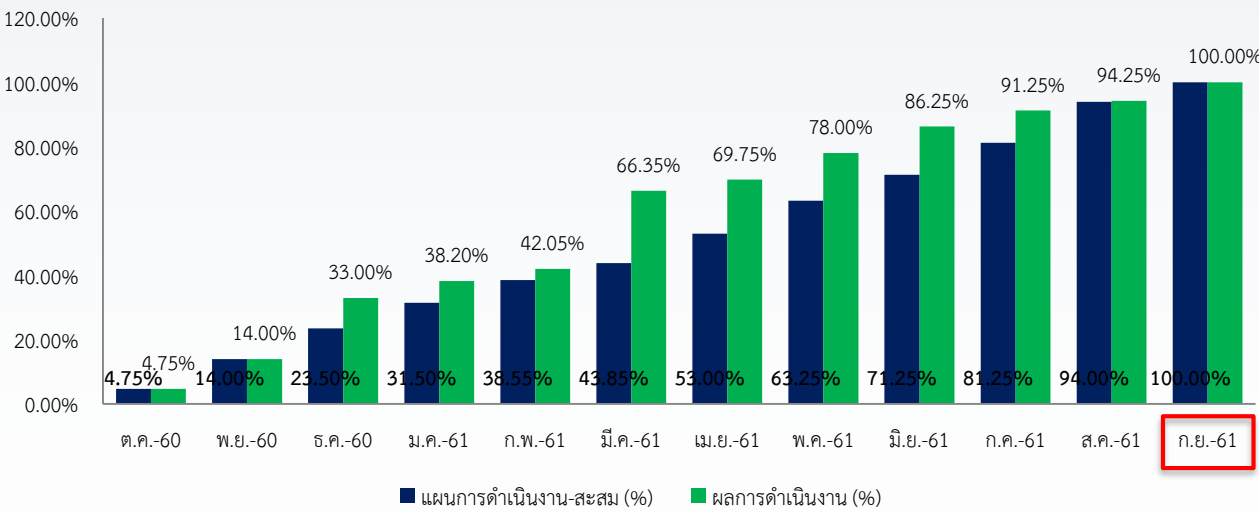
แผน: 100%

ผล: 100%

(ข้อมูล ณ เดือนกันยายน 2561)

สรุปแผน/ผลการดำเนินงานตามตัวชี้วัดโครงการ e-Trade Facilitation

ตัวชี้วัดโครงการ ปีงบประมาณ พ.ศ. 2561	แผน ปี61	ผล ปี61	ผล ปี60	ผล ปี59
1. มีแพลตฟอร์มสำหรับการบริการโครงสร้างพื้นฐานด้าน e-authentication และ/หรือ e-document สำหรับ Trade Facilitation	อย่างน้อย 1 ระบบ	2 ระบบ 	13 เอกสาร (วัตถุดิบทราย)	5 ระบบ (อ้อยและน้ำตาล)
2. จำนวนผู้เข้ารับการอบรมเชิงลึก/กิจกรรม เพื่อยกระดับทักษะฯ	270 คน	370 คน 	447 คน	487 คน
3. จำนวน (ร่าง) หลักเกณฑ์/มาตรฐาน/ข้อเสนอแนะ ที่เอื้อต่อการใช้ประโยชน์ด้านเศรษฐกิจดิจิทัล	2 เรื่อง	4 เรื่อง 	3 เรื่อง	4 เรื่อง
4. ผ่านการตรวจประเมินและปรับแก้ระบบเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยร้ายแรง	อย่างน้อย 2 ระบบ	2 ระบบ 	4 ระบบ	-
5. ร้อยละความพึงพอใจของผู้รับบริการ	ร้อยละ 80	97.57 	ร้อยละ 98	-



ผลการดำเนินงานโครงการ ปี 2561

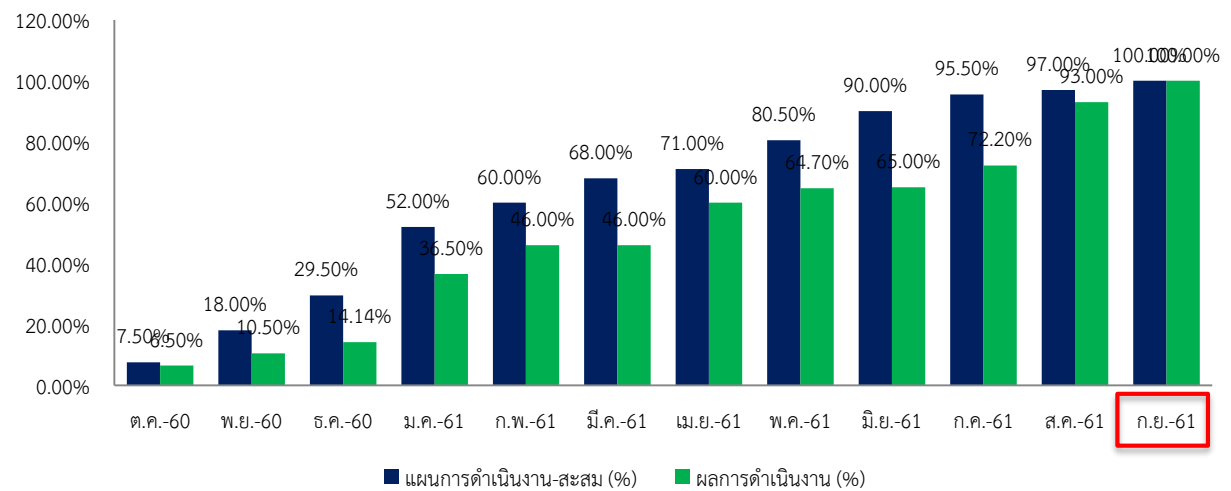


แผน: 100%
 ผล: 100%

(ข้อมูล ณ เดือนกันยายน 2561)

หมายเหตุ: แผนการดำเนินงานโครงการจะมีการทบทวน ปีละ 1 ครั้ง (ช่วงหลังไตรมาสที่ 2)

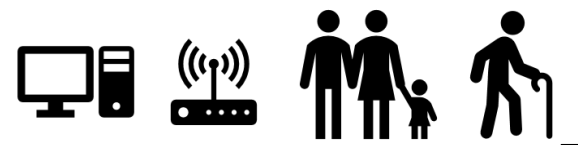
ตัวชี้วัดโครงการ ปีงบประมาณ พ.ศ. 2561	แผน	ผล
1. หลักสูตรที่เหมาะสมกับกลุ่มเป้าหมาย	2 หลักสูตร	2 หลักสูตร
2. จัดทำสื่อ (คลิป กราฟฟิก หนังสือ) และวัสดุประกอบกิจกรรมการเรียนการสอน แบ่งเป็น		
- จำนวนสื่อออนไลน์	5 เรื่อง	> 5 เรื่อง
- จำนวนสื่อประเภทหนังสือ	1 เรื่อง	1 เรื่อง
3. จำนวนผู้เข้าอบรม รวมทั้งสิ้น ไม่น้อยกว่า	3,500 คน	4,116 คน
4. ผู้เข้าอบรมมีความรู้ ความเข้าใจ เพิ่มขึ้นไม่น้อยกว่า	ร้อยละ 80	ร้อยละ 99.17
5. ผู้เข้าอบรมมีความพึงพอใจในการเข้าร่วมอบรม ไม่น้อยกว่า	ร้อยละ 80	ร้อยละ 97.52



โครงการใหม่ในปี 2561

ผลการดำเนินงานโครงการ

แผน: 100%
 ผล: 100 %
 (ข้อมูล ณ เดือนกันยายน 2561)



หมายเหตุ: แผนการดำเนินงานโครงการจะมีการทบทวน ปีละ 1 ครั้ง (ช่วงหลังไตรมาสที่ 2)