

แผนปฏิบัติการยุทธศาสตร์ 6

สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

เป้าหมายของการขับเคลื่อน:

ประชาชนและภาคธุรกิจมีความเชื่อมั่นในการทำธุรกรรมออนไลน์อย่างเต็มรูปแบบ โดยมีระบบรองรับที่ปลอดภัยจากภัยคุกคามไซเบอร์ ดูแลและคุ้มครองข้อมูลส่วนบุคคลให้มีการนำไปใช้ประโยชน์อย่างเหมาะสม ภายในขอบเขตที่ได้รับความยินยอม มีมาตรการเยียวยาความเสียหายแก่ผู้บริโภคอย่างครบวงจรที่สะดวก รวดเร็ว เมื่อเกิดกรณีไม่พึงประสงค์ กำหนดมาตรฐานข้อมูลที่เป็นสากล สอดคล้องกับแนวปฏิบัติที่ได้รับการยอมรับเป็นการทั่วไป ระบบและข้อมูลมีความพร้อมต่อการเชื่อมโยงและใช้ประโยชน์ในการทำธุรกรรมระหว่าง รัฐ เอกชน และข้ามหน่วยงาน ภาครัฐจัดทำชุดกฎหมาย กฎระเบียบที่ทันสมัย ชัดเจน เพื่อรองรับการพัฒนา เศรษฐกิจและสังคม

ตัวชี้วัดของเป้าหมายของยุทธศาสตร์ที่ 6 ในระยะ 5 ปี

เป้าหมายยุทธศาสตร์	เป้าหมายรายปี				
	2560	2561	2562	2563	2564
1. ประชาชนและภาคธุรกิจมีความเชื่อมั่นในการทำธุรกรรมออนไลน์อย่างเต็มรูปแบบ					
1.1 มีผู้ใช้อินเทอร์เน็ตที่ทำธุรกรรมเพิ่มสูงขึ้นต่อเนื่อง และมูลค่า e-Commerce เพิ่มขึ้นไม่น้อยกว่าร้อยละ 4 ต่อปี					
ตัวชี้วัด (1) อัตราการเพิ่มขึ้นของมูลค่าพาณิชย์อิเล็กทรอนิกส์ต่อปี	ร้อยละ 4	ร้อยละ 4	ร้อยละ 4	ร้อยละ 4	ร้อยละ 4
ตัวชี้วัด (2) อัตราการเพิ่มขึ้นของมูลค่าการชำระเงินทางอิเล็กทรอนิกส์ (e-Payments) ต่อปี	เพิ่มขึ้นร้อยละ 2	เพิ่มขึ้นสะสม จากปีก่อน ร้อยละ 2	เพิ่มขึ้นสะสม จากปีก่อน ร้อยละ 3	เพิ่มขึ้น สะสมจากปี ก่อน ร้อยละ 4	เพิ่มขึ้นสะสม จากปีก่อน ร้อยละ 4 (เพิ่มมูลค่า e-Payments ไม่ต่ำกว่า 42,437 พันล้านบาท)
ตัวชี้วัด (3) อัตราการเพิ่มขึ้นของมูลค่าการใช้จ่ายเงินอิเล็กทรอนิกส์ (e-Money) ต่อปี	เพิ่มขึ้นร้อยละ 3	เพิ่มขึ้นสะสม จากปีก่อน ร้อยละ 4	เพิ่มขึ้นสะสม จากปีก่อน ร้อยละ 5	เพิ่มขึ้น สะสมจากปี ก่อน ร้อยละ 4	เพิ่มขึ้นสะสม จากปีก่อน ร้อยละ 4 (มูลค่าของ e-Money)

เป้าหมายยุทธศาสตร์	เป้าหมายรายปี				
	2560	2561	2562	2563	2564
					เพิ่มขึ้น ไม่ต่ำกว่า 13,523 ล้านบาท)
ตัวชี้วัด (4) อัตราการเพิ่มขึ้นของมูลค่าการชำระเงินผ่านบริการ Internet banking ต่อปี	เพิ่มขึ้นร้อยละ 3	เพิ่มขึ้นสะสมจากปีก่อน ร้อยละ 4	เพิ่มขึ้นสะสมจากปีก่อน ร้อยละ 5	เพิ่มขึ้นสะสมจากปีก่อน ร้อยละ 4	เพิ่มขึ้นสะสมจากปีก่อน ร้อยละ 4 (เพิ่มมูลค่าการชำระเงินผ่านบริการ Internet banking 4,776.40 พันล้านบาท)
ตัวชี้วัด (5) อัตราการเพิ่มขึ้นของมูลค่าการชำระเงินผ่านบริการ Mobile banking ต่อปี	เพิ่มขึ้นร้อยละ 5	เพิ่มขึ้นสะสมจากปีก่อน ร้อยละ 5	เพิ่มขึ้นสะสมจากปีก่อน ร้อยละ 6	เพิ่มขึ้นสะสมจากปีก่อน ร้อยละ 8	เพิ่มขึ้นสะสมจากปีก่อน ร้อยละ 6 (เพิ่มมูลค่าการชำระเงินผ่านบริการ Mobile banking 771 พันล้านบาท)
2. มีชุดกฎหมาย กฎระเบียบที่ทันสมัย เพื่อรองรับการพัฒนาเศรษฐกิจและสังคมดิจิทัล					
2.1 ผลักดัน Data Protection Law และปรับแก้ไข Computer Crime Law ให้บังคับใช้ได้ภายใน 3 ปี					
ตัวชี้วัด (6) ความสำเร็จในการปรับปรุงกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ และมีผลบังคับใช้ ในปี พ.ศ. 2560	ดำเนินการแล้วเสร็จและประกาศใช้				
ตัวชี้วัด (7) ความสำเร็จในการพัฒนากฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และมีผลบังคับใช้ ในปี พ.ศ. 2560	ดำเนินการแล้วเสร็จและประกาศใช้				

เป้าหมายยุทธศาสตร์	เป้าหมายรายปี				
	2560	2561	2562	2563	2564
ตัวชี้วัด (8) หน่วยงานภาครัฐ หน่วยงานภาคเอกชน และประชาชนมีความรู้ความเข้าใจเกี่ยวกับกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์และการคุ้มครองข้อมูลส่วนบุคคล	ผลการสำรวจ ปี 2560	เพิ่มขึ้นไม่น้อยกว่า ร้อยละ 70 จากจำนวนผู้เกี่ยวข้อง	เพิ่มขึ้นไม่น้อยกว่า ร้อยละ 75 จากจำนวนผู้เกี่ยวข้อง	เพิ่มขึ้นไม่น้อยกว่า ร้อยละ 80 จากจำนวนผู้เกี่ยวข้อง	เพิ่มขึ้นเป็นร้อยละ 98
2.2 หน่วยงานภาครัฐและภาคเอกชนมีความมั่นคงปลอดภัยทางไซเบอร์ในการรับมือภัยคุกคามทางออนไลน์					
ตัวชี้วัด (9) ความสำเร็จของการจัดตั้งหน่วยงานหรือศูนย์การเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์	มีแผนเฝ้าระวังและรับมือภัยคุกคาม Critical Infrastructure	- มีฐานข้อมูล critical infrastructure ของประเทศ - เกิดหน่วยงานหรือศูนย์เฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์			
ตัวชี้วัด (10) จำนวนเหตุละเมิดความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นในประเทศ	จำนวนเหตุละเมิดความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นในประเทศ ลดลง เมื่อเปรียบเทียบกับปีที่ผ่านมา	จำนวนเหตุละเมิดความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นในประเทศ ลดลง เมื่อเปรียบเทียบกับปีที่ผ่านมา	จำนวนเหตุละเมิดความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นในประเทศ ลดลง เมื่อเปรียบเทียบกับปีที่ผ่านมา	จำนวนเหตุละเมิดความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นในประเทศ ลดลง เมื่อเปรียบเทียบกับปีที่ผ่านมา	จำนวนเหตุละเมิดความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นในประเทศ ลดลง เมื่อเปรียบเทียบกับปีที่ผ่านมา
ตัวชี้วัด (11) ร้อยละของหน่วยงานตามโครงสร้างพื้นฐานที่สำคัญยิ่งยวด (critical infrastructure) ผ่านเกณฑ์มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ	เก็บรวบรวมข้อมูลโดย สป.ตท. หรือ หน่วยงานที่	รายงานสรุปปี 2560	ไม่น้อยกว่า ร้อยละ 80	ไม่น้อยกว่า ร้อยละ 80	ไม่น้อยกว่า ร้อยละ 80

เป้าหมายยุทธศาสตร์	เป้าหมายรายปี					
	2560	2561	2562	2563	2564	
	ได้รับ มอบหมาย					
3. มีมาตรฐานข้อมูลที่เป็นสากล เพื่อรองรับการเชื่อมโยงและใช้ประโยชน์ในการทำธุรกรรม						
3.1 ภาคธุรกิจดำเนินธุรกิจภายในและระหว่างประเทศได้สะดวก รวดเร็ว และต้นทุนทำธุรกรรมผ่านสื่อดิจิทัลลดลง						
ตัวชี้วัด (12) ต้นทุนการทำธุรกรรมผ่านสื่อดิจิทัล (Digital Transaction)		จัดทำแนวทางการเก็บข้อมูล ต้นทุนการทำธุรกรรมผ่านสื่อดิจิทัลแล้วเสร็จ ภายในปี 2561	ต้นทุนการทำธุรกรรมผ่านสื่อดิจิทัล ลดลง เมื่อเปรียบเทียบกับปีที่ผ่านมา	ต้นทุนการทำธุรกรรมผ่านสื่อดิจิทัลลดลง เมื่อเปรียบเทียบกับปีที่ผ่านมา		
ตัวชี้วัด (13) อัตราการเพิ่มขึ้นของมูลค่าพาณิชย์อิเล็กทรอนิกส์ระหว่างภาคธุรกิจด้วยกัน (B2B) ต่อปี	ร้อยละ 2	ร้อยละ 2	ร้อยละ 2	ร้อยละ 2	ร้อยละ 2	
3.2 กระบวนการขอใบอนุญาต มีระยะเวลาที่สั้นลงตามเกณฑ์ของกลุ่มผู้นำในดัชนี Ease of Doing Business ภายใน 2 ปี						
ตัวชี้วัด (14) จำนวนระยะเวลาในการเริ่มต้นธุรกิจ	20 วัน	14 วัน	14 วัน	14 วัน	14 วัน	
3.3 มีมาตรฐานด้านข้อมูลและมาตรฐานเอกสารอิเล็กทรอนิกส์ เพื่อให้สามารถแลกเปลี่ยนและเชื่อมโยงข้อมูลภายในหน่วยงานภาครัฐและระหว่างหน่วยงานภาครัฐและเอกชน						
ตัวชี้วัด (15) จำนวนมาตรฐานข้อมูลที่ประกาศ ส่งเสริมการใช้แลกเปลี่ยนและเชื่อมโยงข้อมูลต่อปี	จำนวน 10 ฉบับ	จำนวน 10 ฉบับ	จำนวน 10 ฉบับ	จำนวน 10 ฉบับ	จำนวน 10 ฉบับ	
ตัวชี้วัด (16) จำนวนหน่วยงานที่มีการแลกเปลี่ยนและเชื่อมโยงข้อมูลภายใต้มาตรฐานที่กำหนดร่วมกัน	ไม่น้อยกว่า ร้อยละ 80 ของหน่วยงานในแต่ละภาคส่วนที่สำคัญ	ไม่น้อยกว่า ร้อยละ 80 ของหน่วยงานในแต่ละภาคส่วนที่สำคัญ	ไม่น้อยกว่า ร้อยละ 80 ของหน่วยงานในแต่ละภาคส่วนที่สำคัญ	ไม่น้อยกว่า ร้อยละ 80 ของหน่วยงานในแต่ละภาคส่วนที่สำคัญ	ไม่น้อยกว่า ร้อยละ 80 ของหน่วยงานในแต่ละภาคส่วนที่สำคัญ	
3.4 อันดับการประเมินวัดดัชนี World Bank's Ease of Doing Business ของไทยดีขึ้นไม่น้อยกว่า 5 อันดับ ภายใน 3 ปี						
ตัวชี้วัดที่ (17) อันดับการประเมินของ World Bank's Ease of Doing Business	อันดับที่ 48	อันดับที่ 46	อันดับที่ 44	อันดับที่ 42	อันดับที่ 40	

กิจกรรมขับเคลื่อน

กิจกรรมที่ 1 การติดตามและเฝ้าระวังระบบโครงสร้างพื้นฐานที่จำเป็นอย่างยิ่งยวด (Critical Infrastructure)

1.1 แนวทางการดำเนินการ

ระบุและทบทวนรายชื่อหน่วยงานที่อยู่ในกลุ่มโครงสร้างพื้นฐานที่มีความจำเป็นอย่างยิ่งยวด (critical infrastructure) เพื่อบริหารจัดการและลดความเสี่ยง กำหนดหน้าที่ของผู้ดูแลระบบที่ต้องเฝ้าระวังและมีมาตรการดำเนินการเมื่อเกิดปัญหาภัยคุกคามไซเบอร์อย่างทันที่และมีประสิทธิภาพ จัดให้มีแนวทางการสร้างภูมิคุ้มกันภัยคุกคามไซเบอร์แก่หน่วยงานและประชาชนทั่วไป ให้เกิดการเรียนรู้และตระหนักถึงภัยคุกคามการลดความเสี่ยง และสร้างความปลอดภัยเมื่อมีการใช้งานเทคโนโลยีดิจิทัลด้วยการขจัดจุดอ่อนที่จะชักนำภัยไซเบอร์เข้าสู่ระบบโดยไม่รู้ตัว

1.2 ผลลัพธ์โครงการ

ระบบการทำงานของหน่วยงานได้รับการปกป้อง เตือนภัย ข้อมูลที่หน่วยงานดูแล ครอบครอง หรือเป็นเจ้าของได้รับการดูแลอย่างเหมาะสม ไม่ถูกนำไปใช้ ประโยชน์ในทางมิชอบ ระบบดำเนินการได้อย่างราบรื่น ปราศจากอุปสรรคและความเสี่ยงจากภัยคุกคามที่จะก่อให้เกิดความเสียหายทั้งทางทรัพย์สินหรือชีวิต

กิจกรรมที่ 2 เพิ่มบทบาทการทำธุรกรรมออนไลน์

2.1 แนวทางการดำเนินการ

จัดเตรียมระบบรองรับอย่างครบวงจร มีมาตรการดูแลระบบให้ปลอดภัย โดยเฉพาะระบบการชำระเงิน และระบบอื่นๆ ปกป้องและคุ้มครองข้อมูลที่หมุนเวียนในระบบให้มีการนำไปใช้อย่างเหมาะสม ไม่ละเมิดข้อมูลส่วนบุคคลสร้างกลไกในการเฝ้าระวัง ลดความเสี่ยง และระงับเหตุเมื่อมีการฉ้อโกงทางออนไลน์ จัดทำกระบวนการรับแจ้งเหตุ มาตรการเยียวยาผู้ได้รับผลกระทบ และ/หรือความเสียหาย มีแนวทางการระงับข้อพิพาทที่สะดวก รวดเร็ว ไม่ซับซ้อน

2.2 ผลลัพธ์โครงการ

ประชาชนมีความเชื่อมั่น และเปลี่ยนรูปแบบการทำธุรกรรมมาสู่ระบบออนไลน์ที่อำนวยความสะดวก และมั่นใจในความปลอดภัย สถิติและมูลค่าการฉ้อโกงออนไลน์และจำนวนข้อพิพาทที่ขึ้นสู่ศาลลดลง

กิจกรรมที่ 3 ปฏิรูประบบกฎหมายที่เน้นการส่งเสริมและสนับสนุนการพัฒนาดิจิทัล ยกเลิกกฎหมายที่เป็นอุปสรรคต่างๆ

3.1 แนวทางการดำเนินการ

บูรณาการกฎหมายทั้งระบบ ด้วยการทบทวนกฎหมาย กฎ ระเบียบ ที่มีอยู่ในปัจจุบัน จัดกลุ่มกฎหมายที่ต้องบัญญัติขึ้นใหม่ ปรับปรุงกฎหมายบางฉบับ ยกเลิกกฎหมายที่เป็นอุปสรรค โดยมุ่งเน้นให้

กฎหมายนั้นมีเนื้อหาที่สอดคล้องกับแนวปฏิบัติสากล ตอบสนองต่อความต้องการของผู้มีส่วนเกี่ยวข้อง เพื่อส่งเสริมและสนับสนุนในการสร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

3.2 ผลลัพธ์โครงการ

ผู้มีส่วนเกี่ยวข้องเกิดความเชื่อมั่นในการดำเนินการใดๆ ที่เกี่ยวข้องกับการดิจิทัล เมื่อกฎหมายมีบทบัญญัติที่ชัดเจน กำหนดสิทธิ หน้าที่ และความรับผิดชอบของแต่ละฝ่ายอย่างครบถ้วน ในขณะเดียวกันบรรเทาและแก้ไขให้กฎหมายไม่เป็นอุปสรรคขัดขวางการใช้งานดิจิทัลอีกต่อไป

กิจกรรมที่ 4 การกำหนดมาตรฐานเพื่อการเชื่อมโยงข้อมูล

4.1 แนวทางการดำเนินการ

กำหนดหน่วยงานที่รับผิดชอบในการดูแลและจัดทำมาตรฐานต่างๆ ที่จำเป็นและเกี่ยวข้องในการส่งเสริมสนับสนุนการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมภายใต้เงื่อนไขว่ามาตรฐานนั้นจะไม่ส่งผลกระทบต่อมีการเชื่อมโยงข้อมูลระบบต่างๆ ในภาพรวม เพื่อให้เกิดการบูรณาการการใช้ข้อมูลระหว่างหน่วยงานภาครัฐและระหว่างหน่วยงานภาครัฐและเอกชน และหน่วยงานต่างๆ สามารถอ้างอิงนำมาตรฐานนั้นไปปรับใช้ได้ อย่างเหมาะสมในรูปแบบเดียวกัน

4.2 ผลลัพธ์โครงการ

เกิดการเชื่อมโยงข้อมูลระหว่างหน่วยงานรัฐกับรัฐ และขยายผลไปสู่การเชื่อมโยงข้อมูลระหว่างรัฐกับเอกชน สามารถบริหารจัดการข้อมูลที่น่าไปสู่การกำหนดนโยบายที่ตอบสนองความต้องการของภาคเอกชน และภาคประชาชนได้อย่างถูกต้อง ทัวถึง เป็นธรรม และทันท่วงที ไม่เกิดปัญหาการให้ความช่วยเหลือที่ซ้ำซ้อนหรือไม่ตรงกับกลุ่มเป้าหมาย ลดต้นทุนในการเดินทาง ลดปริมาณเอกสารในการดำเนินการ ประหยัดเวลาด้วยการกรอกข้อมูลครั้งเดียว สามารถติดต่อราชการโดยไม่ถูกจำกัดด้วยเวลาและสถานที่อีกต่อไป

กิจกรรมที่ 5 การบริหารจัดการภัยคุกคามไซเบอร์

5.1 แนวทางการดำเนินการ

มีกฎหมายที่ดูแลเรื่องภัยคุกคามไซเบอร์ทั้งระบบ ซึ่งมีสภาพบังคับอย่างเข้มข้นและจริงจัง หน่วยงานที่ดูแลเกี่ยวกับโครงสร้างพื้นฐานสาธารณะทั้งหมด รวมถึงหน่วยงานรัฐที่ดูแลเกี่ยวกับความมั่นคงและเศรษฐกิจ การให้บริการสาธารณะและอื่นๆ มีหน้าที่ต้องจัดเตรียมระบบที่รองรับภัยคุกคามไซเบอร์ มีการดำเนินการทดสอบระบบอย่างสม่ำเสมอและต่อเนื่อง เตรียมความพร้อมรับมือด้วยการฝึกซ้อมจากสถานการณ์สมมุติ พร้อมทั้งกำหนดมาตรการในการดำเนินการและแผนรองรับหากเกิดเหตุการณ์ไม่พึงประสงค์ขึ้น สร้างความตระหนักแก่ประชาชน

5.2 ผลลัพธ์โครงการ

มาตรการเฝ้าระวัง การป้องกันภัยคุกคาม ตามมาตรฐานสากล อย่างบูรณาการ ช่วยลดความเสี่ยงและ
ความเสียหายจากภัยคุกคามไซเบอร์การติดตามและเฝ้าระวังระบบโครงสร้างพื้นฐานที่จำเป็นอย่างยิ่งยวด
(Critical Infrastructure)

ตารางสรุปกิจกรรมยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

กิจกรรม	แนวทางการดำเนินงาน	ผลลัพธ์		หน่วยงานเจ้าภาพหลัก และสนับสนุน
		1 ปี 6 เดือน Digital Foundation (มค. 2560 - มิ.ย. 2561)	5 ปี Digital Thailand : Inclusion (กค. 2561 - ธ.ค. 2564)	
กิจกรรมที่ 1 การติดตามและ เฝ้าระวังระบบโครงสร้าง พื้นฐานที่จำเป็นอย่างยั่งยืน (Critical Infrastructure)	<p>1.1 ตรวจสอบความพร้อมในการบริหารจัดการความเสี่ยง</p> <p>1.2 ทบทวนและจัดกลุ่มรายชื่อระบบที่จัดว่าเป็น critical infrastructure</p> <p>1.3 จัดทำแผนปฏิบัติการเพื่อรองรับสถานะฉุกเฉิน</p> <p>1.4 สร้างความตระหนักและการรับรู้ให้กับหน่วยงานทั้งภาครัฐ ภาคเอกชน และประชาชนได้เข้าใจและเล็งเห็นถึงความสำคัญในการป้องกันและเฝ้าระวังภัย</p>	<p>1.1.1 ฐานข้อมูล critical infrastructure ของประเทศ</p> <p>1.3.1 ระบบสำรองข้อมูลในภาวะฉุกเฉิน</p> <p>1.3.2 แผนเฝ้าระวังและรับมือภัยคุกคาม Critical Infrastructure</p> <p>1.3.3 ระบบป้องกันภัยและสกัดปัญหา</p> <p>1.4.1 หน่วยงานและประชาชนเกิดความตระหนักและเห็นถึงความสำคัญและความจำเป็นในการใช้ระบบดิจิทัลอย่างรู้เท่าทันและปลอดภัยมากขึ้น</p>	<p>โครงสร้างพื้นฐานที่จำเป็นอย่างยั่งยืน (Critical Infrastructure) มีความคล่องตัวในการบริหารจัดการปัญหาและป้องกันความเสี่ยง ใช้เวลาดลดลงในการระงับเหตุ ลดปริมาณความเสียหายหยุดยั้งภัยคุกคาม และดำเนินการทางกฎหมายกับผู้กระทำผิด</p>	<p>ธนาคารแห่งประเทศไทย</p> <p>สถาบันการเงิน</p> <p>กระทรวงมหาดไทย</p> <p>กระทรวงกลาโหม</p> <p>กระทรวงสาธารณสุข</p> <p>กระทรวงพลังงาน</p> <p>กระทรวงคมนาคม</p> <p>สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ</p> <p>สำนักงานตำรวจแห่งชาติ</p>
กิจกรรมที่ 2 เพิ่มบทบาทการ ทำธุรกรรมออนไลน์	<p>2.1 สร้างกลไกดูแลเรื่องการกระทำผิดออนไลน์</p>	<p>2.1.1 มีระบบรองรับที่ปลอดภัยคุ้มครองข้อมูลที่หมุนเวียนในระบบอย่างเหมาะสม</p>	<p>มูลค่าและปริมาณการทำธุรกรรมออนไลน์สูงขึ้นจนทดแทนการทำธุรกรรมในรูปแบบเดิม</p>	<p>กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมดูแลเรื่องโครงสร้างพื้นฐานและจัดให้มีระบบที่รองรับการทำธุรกรรมออนไลน์</p>

กิจกรรม	แนวทางการดำเนินงาน	ผลลัพธ์		หน่วยงานเจ้าภาพหลัก และสนับสนุน
		1 ปี 6 เดือน Digital Foundation (ม.ค. 2560 - มิ.ย. 2561)	5 ปี Digital Thailand : Inclusion (กค. 2561 - ธ.ค. 2564)	
	<p>2.2 พัฒนาระบบรองรับการดำเนินงานเพิ่มเติม รวมทั้งปรับปรุงระบบที่มีอยู่ให้มีความปลอดภัยเพิ่มขึ้น</p> <p>2.3 พัฒนาระบบการรับแจ้งเหตุ กำหนดมาตรการเยียวยาผู้บริโภคที่ได้รับผลกระทบจากข้อพิพาทการฉ้อโกงออนไลน์</p> <p>2.4 สร้างความรู้ ความเข้าใจ ในเทคโนโลยีดิจิทัลแก่ผู้เกี่ยวข้องในการปฏิบัติหน้าที่</p>	<p>2.3.1 รายงานการศึกษาแนวทางการระงับข้อพิพาทที่สะดวก รวดเร็ว ไม่ซับซ้อน</p> <p>2.3.2 มีมาตรการให้การดูแลและเยียวยาผู้ได้รับผลกระทบจากข้อพิพาทการฉ้อโกงออนไลน์</p>	<p>2.4.1 เจ้าหน้าที่ผู้เกี่ยวข้องในทุกภาคส่วนมีความรู้และเข้าใจถึงรูปแบบและลักษณะของเทคโนโลยีดิจิทัลที่เปลี่ยนแปลงตลอดเวลาซึ่งอยู่ภายใต้บริบทของกฎหมายที่เกี่ยวข้องและปรับใช้กฎหมายได้ถูกต้องตามเจตนารมณ์</p>	และประสานงานกับหน่วยงานที่เกี่ยวข้อง
กิจกรรมที่ 3 ปฏิรูประบบกฎหมายที่เน้นการส่งเสริมและสนับสนุนการพัฒนาดิจิทัล ยกเลิกกฎหมายที่เป็นอุปสรรคต่างๆ	<p>3.1 บูรณาการกฎหมายทั้งระบบ ด้วยการทบทวนกฎหมาย กฎ ระเบียบ ที่มีอยู่ในปัจจุบัน และจัดกลุ่มกฎหมายที่ต้องบัญญัติขึ้นใหม่ ปรับปรุง หรือยกเลิก</p> <p>3.2 ทบทวนกฎหมายที่เป็นอุปสรรค และบัญญัติกฎหมายเพิ่มเติมที่เอื้อต่อการพัฒนา</p>	<p>3.2.1 ชุดกฎหมายที่ได้รับการปรับปรุง</p>	ชุดกฎหมายที่ครบถ้วน ชัดเจน บังคับใช้อย่างมีประสิทธิภาพ	กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ประสานงานกับหน่วยงานที่เกี่ยวข้องที่รับผิดชอบดูแลกฎหมายแต่ละฉบับ

กิจกรรม	แนวทางการดำเนินงาน	ผลลัพธ์		หน่วยงานเจ้าภาพหลัก และสนับสนุน
		1 ปี 6 เดือน Digital Foundation (ม.ค. 2560 - มิ.ย. 2561)	5 ปี Digital Thailand : Inclusion (กค. 2561 - ธ.ค. 2564)	
	เศรษฐกิจและสังคมดิจิทัลจากกฎหมายที่มีอยู่ ณ ปัจจุบัน เพื่อกำหนดกรอบปฏิบัติที่ เหมาะสมกับบริบทของการพัฒนาดิจิทัลเพื่อ เศรษฐกิจและสังคมในภาพรวม 3.3 ติดตามและปรับปรุงกฎหมายให้ทันสมัย อย่างต่อเนื่อง	3.2.2 กฎหมายฉบับใหม่ที่เหมาะสม ต่อบริบทการขับเคลื่อนประเทศ		
กิจกรรมที่ 4 การกำหนด มาตรฐานเพื่อการเชื่อมโยง ข้อมูล	4.1 ตรวจสอบ รวบรวม และจัดกลุ่มมาตรฐาน ที่จำเป็นเร่งด่วน 4.2 จัดทำมาตรฐานต่างๆ ที่จำเป็นเพิ่มเติม ซึ่ง ต้องไม่ส่งผลกระทบต่อเชื่อมโยงข้อมูลผ่าน ระบบต่างๆ ในภาพรวม 4.3 บูรณาการเชื่อมโยงข้อมูล เพื่อวิเคราะห์ และนำไปใช้ประโยชน์ ลดต้นทุน อำนวยความ สะดวกการใช้ข้อมูลระหว่างหน่วยงานภาครัฐ และระหว่างหน่วยงานภาครัฐกับเอกชน 4.4 ติดตามความคืบหน้าเพื่อจัดให้มีมาตรฐาน เพิ่มเติม และปรับปรุงมาตรฐานเดิมให้ทันสมัย อย่างต่อเนื่อง	4.1.1 รายงานสรุปกลุ่มมาตรฐาน จำเป็นเร่งด่วนต่อการพัฒนาดิจิทัล เพื่อเศรษฐกิจและสังคม 4.2.1 ชุดมาตรฐานที่ปรับปรุง และ ชุดมาตรฐานใหม่เพิ่มเติมจากเดิม 4.3.1 มาตรการ/แนวปฏิบัติการ บูรณาการข้อมูลระหว่างหน่วยงาน ภาครัฐด้วยกัน 4.4.1 ชุดมาตรฐานที่เหมาะสม สอดคล้องกับบริบทความ เปลี่ยนแปลง	4.2.2. มีชุดมาตรฐานที่จำเป็น ครบถ้วนและสอดคล้องกับ มาตรฐานสากล 4.3.2 มาตรการ/แนวปฏิบัติ การบูรณาการข้อมูลระหว่าง หน่วยงานภาครัฐกับเอกชน 4.4.2 ชุดมาตรฐานที่เหมาะสม สอดคล้องกับบริบทความ เปลี่ยนแปลง	กระทรวงดิจิทัลเพื่อ เศรษฐกิจและสังคม ประสานหน่วยงานเพื่อ กำหนดและจัดทำ มาตรฐานที่จำเป็นเพื่อ นำไปใช้ในรูปแบบเดียวกัน
กิจกรรมที่ 5 การบริหารจัดการ ภัยคุกคามไซเบอร์	5.1 จัดวางระบบเฝ้าระวังและป้องกันภัย คุกคามทางไซเบอร์อย่างมีประสิทธิภาพ	5.1.1 ระบบเฝ้าระวังและป้องกันภัย คุกคามทางไซเบอร์	5.1.2 ระบบเฝ้าระวังและป้องกัน ภัยคุกคามทางไซเบอร์ที่ทันสมัย และชาญฉลาด	ทุกหน่วยงานทั้งภาครัฐ ภาคเอกชน ภาควิชาการ และภาคประชาชน

กิจกรรม	แนวทางการดำเนินงาน	ผลลัพธ์		หน่วยงานเจ้าภาพหลัก และสนับสนุน
		1 ปี 6 เดือน Digital Foundation (มค. 2560 - มิ.ย. 2561)	5 ปี Digital Thailand : Inclusion (กค. 2561 - ธ.ค. 2564)	
	<p>5.2 สร้างกลไกการเฝ้าระวังภัยคุกคามไซเบอร์อย่างครบวงจร ทันต่อภัยและมีประสิทธิภาพ</p> <p>5.3 จัดเตรียมหน่วยงานที่ดูแลและรับผิดชอบในการดำเนินการที่เกี่ยวข้องกับการบริหารจัดการปัญหาภัยคุกคามไซเบอร์</p> <p>5.4 สร้างความตระหนักและการรับรู้ให้กับประชาชนได้เข้าใจและเห็นถึงความสำคัญในการป้องกันและเฝ้าระวังภัยทางไซเบอร์</p>	<p>5.2.1 (ร่าง) กฎหมายความมั่นคงปลอดภัยทางไซเบอร์ ที่กำหนดสิทธิหน้าที่ และความรับผิดชอบของผู้เกี่ยวข้อง ได้อย่างครบถ้วน ชัดเจน</p> <p>5.3.1 หน่วยงานกลางที่ดูแลและรับผิดชอบในการดำเนินการที่เกี่ยวข้องกับการบริหารจัดการปัญหาภัยคุกคามไซเบอร์</p> <p>5.4.1 ประชาชนมี ความตระหนักและเห็นถึงความสำคัญมากขึ้นผ่านสื่อมวลชน</p>	<p>5.2.2 มีกฎหมายที่ดูแลเรื่องภัยคุกคามไซเบอร์ทั้งระบบ มีสภาพบังคับอย่างเข้มข้นและจริงจัง</p> <p>5.2.3 จำนวนการถูกโจมตีทางไซเบอร์ของหน่วยงานรัฐและเอกชนลดลง และระยะเวลาการกู้คืนเร็วขึ้น</p>	

