นโยบายความมั่นคงปลอดภัยของระบบสารสนเทศภาครัฐ

นางสาวรัตนา จรูญศักดิ์สิทธิ์

ผอ.กลุ่มงานผลักดันธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

หัวข้อการบรรยาย

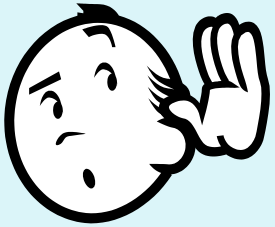
- กฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- การยกระดับมาตรการรักษาความมั่นคงปลอดภัย

กฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

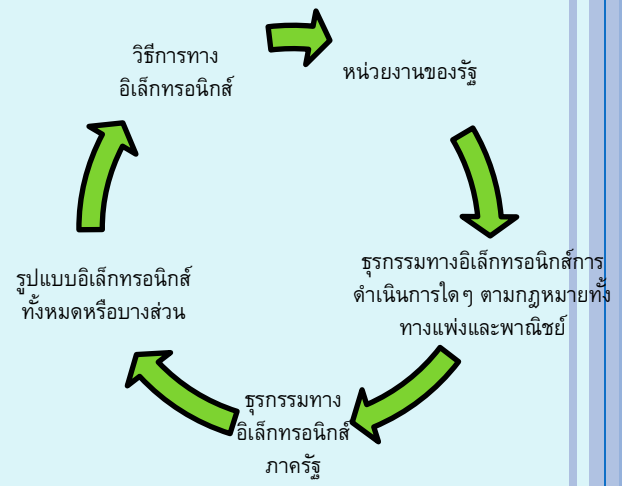
กฎหมายที่เกี่ยวข้อง

กฎหมายที่เกี่ยวข้อง

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐	พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๑
ให้พนักงานเจ้าหน้าที่ เป็นพนักงานฝ่ายปกครองหรือตำรวจชั้นผู้ใหญ่ตามประมวลกฎหมายวิธีพิจารณาความอาญา มีอำนาจรับคำร้องทุกข์หรือรับคำกล่าวโทษ และมีอำนาจในการสืบสวนสอบสวนเฉพาะความผิดตามพระราชบัญญัตินี้	พระราชบัญญัตินี้ให้ใช้บังคับแก่ธุรกรรมในการดำเนินงานของรัฐตามที่กำหนดในหมวด ๔ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด



ขอบเขตการดำเนินงาน



หน่วยงานของรัฐ

กระทรวง ทบวง กรม ส่วนราชการที่เรียกชื่ออย่างอื่นและมีฐานะเป็นกรม ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจที่ตั้งขึ้นโดยพระราชบัญญัติหรือพระราชกฤษฎีกา และให้หมายความรวมถึงนิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในการใด ๆ

วิธีการทาง E

วิธีการสร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแต่บางส่วน เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข การส่งข้อความสั้น หรือโทรสาร รวมทั้งการเผยแพร่ผ่าน เว็บไซต์ของหน่วยงาน

ธุรกรรมฯ ภาครัฐ

การจัดทำคำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใดๆตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ

มาตรการด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเทศ ภายใต้พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

พระราชกฤษฎีกา

มาตรา ๓๕

พรฎ.กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙

มาตรา ๒๕

พรฎ. ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

พรฎ.กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

เงื่อนไขตาม พรบ.ธุรกรรมฯ

มาตรา ๓๕ คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา ให้นำพระราชบัญญัตินี้มาใช้บังคับและให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด

หน่วยงานของรัฐต้องจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลบังคับได้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

มุ่งเน้น : การดำเนินงานของหน่วยงานของรัฐ

เนื้อหาอย่างน้อยต้องประกอบด้วย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

ปรับแก้ไข ประกาศ ข้อ ๑๔

เน้นการแสดงความรับผิดชอบของผู้บริหารระดับสูง

หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิด ความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่องแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

มุ่งเน้น : การรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์

สาระสำคัญ

- เก็บรวบรวมอย่างจำกัด
- จัดเก็บตามอำนาจหน้าที่
- ระบุวัตถุประสงค์ในการจัดเก็บ
- ระบุข้อจำกัดในการนำข้อมูลไปใช้
- การรักษาความมั่นคงปลอดภัย
- ระบุการมีส่วนร่วมของเจ้าของข้อมูล
- ระบุความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล

พรฎ.ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ และ บัญชีแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

(ร่าง) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหรือประเภทของหน่วยงานหรือองค์กรหรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ

เงื่อนไขตาม พรบ.ธุรกรรมฯ

มาตรา ๒๕ ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิฐานว่าเป็นวิธีการที่เชื่อถือได้

แนวทางสำคัญ : การบริหารความเสี่ยงของระบบสารสนเทศ

การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

พรฎ.กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

มาตรา ๕
หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เนื้อหาอย่างน้อยต้องประกอบด้วย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

สิ่งที่หน่วยงานของรัฐต้องจัดทำ :

๑. นโยบายในการรักษาความมั่นคงปลอดภัย

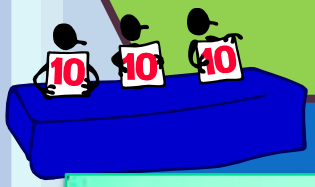
๒. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

๓. แผนสำรองระบบสารสนเทศและแผนเตรียมความพร้อมกรณีฉุกเฉิน

๔. คำสั่งแต่งตั้ง และการกำหนดความรับผิดชอบตามนโยบายและแนวปฏิบัติ

พรฎ.กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

มาตรา ๗
หน่วยงานของรัฐต้องจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลบังคับได้



คณะกรรมการธุรกรรมฯ กำหนด :

๑. ผู้ทำหน้าที่ตรวจประเมินนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

๒. ขั้นตอนปฏิบัติในการจัดส่งนโยบายและแนวปฏิบัติฯ เพื่อขอความเห็นชอบ

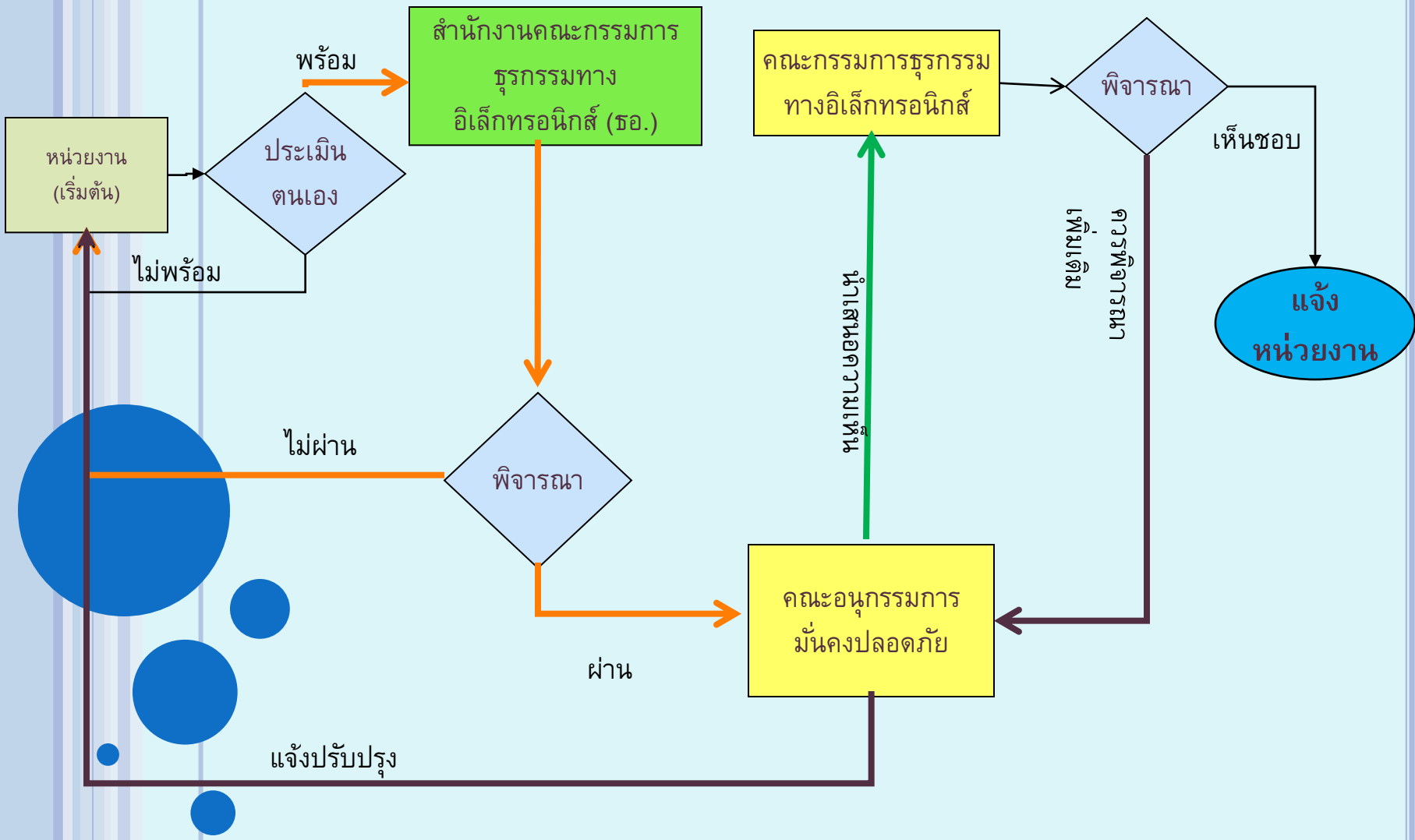
๓. แนวทางการตรวจประเมินความครบถ้วนการดำเนินงานตามที่ประกาศฯ กำหนด

คณะกรรมการธุรกรรมฯ มอบหมาย

๑. สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบในการกลั่นกรองตรวจสอบรายละเอียดนโยบายและแนวปฏิบัติของหน่วยงาน และทำความเห็นเสนอคณะอนุกรรมการที่เกี่ยวข้องเพื่อพิจารณาในเบื้องต้น

๒. คณะอนุกรรมการความมั่นคงปลอดภัยพิจารณาให้ความเห็นเบื้องต้น เสนอต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

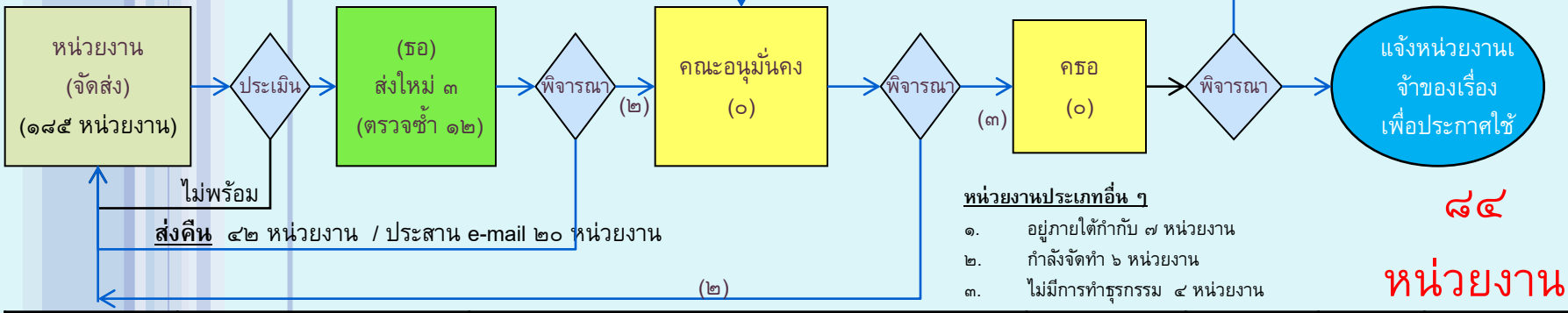
ขั้นตอนปฏิบัติในการจัดส่งนโยบายและแนวปฏิบัติฯ



สรุปผลการดำเนินงานเกี่ยวกับการจัดทำแนวนโยบายและแนวปฏิบัติฯ

ปีงบประมาณ พ.ศ. ๒๕๕๓ - พ.ศ. ๒๕๕๘

(ปรับปรุงล่าสุด ณ วันที่ ๓๑ ตุลาคม ๒๕๕๗)



หน่วยงานประเภทอื่น ๆ

๑. อยู่ภายใต้กำกับ ๗ หน่วยงาน
๒. กำลังจัดทำ ๖ หน่วยงาน
๓. ไม่มีการทำธุรกรรม ๔ หน่วยงาน

๘๔ หน่วยงาน

ปีงบประมาณ	จำนวนที่จัดส่ง		จำนวนที่ผ่าน (หน่วยงาน) แยกตามปี						รอเสนอ คธอ	รอเสนออนุมั่นคง	ส่งคืน	หมายเหตุ
	ทั้งหมด	แยก ๖ เดือน	๒๕๕๓	๒๕๕๔	๒๕๕๕	๒๕๕๖	๒๕๕๗	๒๕๕๘				
๒๕๕๓	๓	๓	๑	๑	๑							หน่วยงานประสานส่งกลับมาตรวจอย่างต่อเนื่อง
๒๕๕๔	๘๕	๕๒		๑๓	๑๓	๓	๓	๑		๑	๗	
		๓๓		๒	๗	๖	๒	๓	๑		๑๒	
๒๕๕๕	๓๙	๒๗			๒	๔	๔		๑	๑	๙	
		๑๒				๓	๓				๖	
๒๕๕๖	๒๓	๑๔					๒	๑	๑		๖	
		๙					๓	๔			๑	
๒๕๕๗	๓๒	๒					๑					
		๓๐						๒			๑	
๒๕๕๘	๓	๓										
รวม	๑๘๕		๑	๑๖	๒๓	๑๖	๑๘	๑๐	๓	๒	๔๒	
			๘๔									

แบบประเมินประกอบการพิจารณาการดำเนินงานฯ ตามมาตรา ๗

แบบประเมินประกอบการพิจารณาการดำเนินงานตาม
แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา ๗ ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

ชื่อหน่วยงานผู้นำเสนอ .....
เอกสารประกอบการพิจารณา .....(สามารถแนบเพิ่มเติมได้)
.....

หมายเหตุ : กรณีที่กรรมการธุรกรรมทางอิเล็กทรอนิกส์ หรืออนุกรรมการมีความเกี่ยวข้องกับข้อเสนอที่กำลังพิจารณา ต้องแสดงตนเพื่อหลีกเลี่ยงปัญหาการมีผลประโยชน์ทับซ้อน (Conflicts of Interest)

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก ธอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจาก อนุกรรมการความมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
๑	**กำหนดคำนิยาม**				
	(๑) ผู้ใช้งาน				
	(๒) สิทธิของผู้ใช้งาน				
	(๓) สินทรัพย์				
	(๔) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ				
	(๕) ความมั่นคงปลอดภัยด้านสารสนเทศ				
	(๖) เหตุการณ์ด้านความมั่นคงปลอดภัย				
	(๗) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด				
	(๘) คำนิยามอื่น ๆ ตามความต้องการขององค์กร				
๒	**หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน เป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหาดังต่อไปนี้**				
	(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ				
	(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง				
	(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ				

(ตัวอย่าง) แบบประเมินหน้าแรก

ระบุเอกสารทุกรายการ
เรียงลำดับ ๑, ๒,....

แบบประเมินประกอบการ
แนวนโยบายและแนวปฏิบัติ ในการรักษา
ตามมาตรา ๗ ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิ

ชื่อหน่วยงานผู้นำเสนอ กรมสรรพากร กระทรวงการคลัง

เอกสารประกอบการพิจารณา
๑. ร่างนโยบายความมั่นคงปลอดภัยสารสนเทศของกรมสรร
๒. ร่างระเบียบกรมสรรพากรว่าด้วยการบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. ๒๕๕...
๓. ร่างระเบียบกรมสรรพากรว่าด้วยการใช้ระบบคอมพิวเตอร์ของกรมสรรพากรอย่างปลอดภัย พ.ศ. ๒๕๕...
๔. ร่างระเบียบกรมสรรพากรว่าด้วยการใช้ระบบคอมพิวเตอร์เพื่อรับส่งหนังสือและข่าวสารทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕...
๕. ร่างระเบียบกรมสรรพากรว่าด้วยการใช้ระบบเครือข่ายสื่อสารคอมพิวเตอร์ พ.ศ. ๒๕๕...
๖. แผนกู้เหตุฉุกเฉิน
๗. หนังสือที่ กค ๐๗๑๘/ทท/ว ๓๔๕๔ ลงวันที่ ๘ ตุลาคม ๒๕๕๑ และหนังสือที่ กค ๐๗๑๘/ทท/ว ๑๑๒ ลงวันที่ ๑๓ มกราคม ๒๕๕๒

หมายเหตุ : กรณีที่กรรมการธุรกรรมทางอิเล็กทรอนิกส์ หรืออนุกรรมการมีความเกี่ยวข้องกับข้อเสนอที่กำลังพิจารณา ต้องแสดงตนเพื่อหลีกเลี่ยงปัญหาการมีผลประโยชน์ทับซ้อน (Conflicts of Interest)

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก ธอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจากอนุกรรมการมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
๑	กำหนดคำนิยาม				
	(๑) ผู้ใช้งาน	ผ่าน	หมายเลข ๒ หน้า ๒ ข้อ ๔ หมายเลข ๓ หน้า ๑ ข้อ ๓ หมายเลข ๕ หน้า ๑ ข้อ ๓	เห็นด้วย	
	(๒) สิทธิของผู้ใช้งาน	ผ่าน	หมายเลข ๒ หน้า ๒ ข้อ ๔	เห็นด้วย	

(ตัวอย่าง) แบบประเมินหน้าสุดท้าย

โปรดระบุเพื่อรับทราบ ☐ กรณีหน่วยงานมีเอกสารที่เป็นความลับ ไม่จำเป็นต้องจัดส่งเอกสาร แต่ให้นำมาชี้แจงประกอบการพิจารณาของคณะกรรมการ

ขอรับรองว่าข้อความที่แจ้งไว้ในแบบฟอร์มนี้ถูกต้อง เป็นความจริงทุกประการ และสอดคล้องตามแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยของหน่วยงานภาครัฐ ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ลงชื่อ ..... (ผู้บริหารสูงสุด/ผู้ที่ได้รับมอบอำนาจ)
(.....)
ตำแหน่ง .....
ลงวันที่ .....

เรียน ผู้อำนวยการสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ความเห็นของผู้ประเมินเบื้องต้น ☑ เห็นสมควรให้ความเห็นชอบ ☐ เห็นสมควรให้มีการปรับแก้ (ระบุรายละเอียด)

.....
.....
.....

หลังจากหน่วยงาน ประเมินตนเองเสร็จสิ้น ให้ผู้บริหารสูงสุด / ผู้ที่ได้รับมอบอำนาจ ลงนามรับรอง ก่อนส่งให้สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ตำแหน่ง ผู้อำนวยการกลุ่มงานผลักดันธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
ลงวันที่ .....

การยกระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

มาตรา ๒๕

มาตรา ๓๕

พิจารณาตาม

-หลักเกณฑ์การประเมินระดับผลกระทบ

-ระดับความเสี่ยงที่ได้จากการประเมิน

-หน่วยงาน Critical Infrastrucure

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

มาตรการวิธีการแบบปลอดภัย แบ่งออกเป็น ๑๑ กลุ่ม ได้แก่

(๑) นโยบายด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

(๒) โครงสร้างการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

(๓) การบริหารจัดการสินทรัพย์สารสนเทศ

(๔) การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

(๕) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

(๖) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

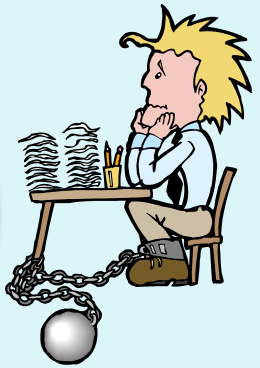
(๗) การควบคุมการเข้าถึงระบบเครือข่าย คอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

(๘) การจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๙) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

(๑๐) การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

(๑๑) การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใดๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ



ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

ธุรกรรมทางอิเล็กทรอนิกส์ที่ต้องใช้วิธีการแบบปลอดภัยในระดับเคร่งครัด มีดังนี้

- ธุรกรรมทางอิเล็กทรอนิกส์ด้านการชำระเงินทางอิเล็กทรอนิกส์ตามพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑
- ธุรกรรมทางอิเล็กทรอนิกส์ด้านการเงินของธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน
- ธุรกรรมทางอิเล็กทรอนิกส์ด้านประกันภัย ตามกฎหมายว่าด้วยประกันชีวิตและประกันชีวิตและประกันวินาศภัย
- ธุรกรรมทางอิเล็กทรอนิกส์ด้านหลักทรัพย์ของผู้ประกอบธุรกิจหลักทรัพย์ตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์
- ธุรกรรมทางอิเล็กทรอนิกส์ที่จัดเก็บรวบรวม และให้บริการข้อมูลของบุคคลหรือทรัพย์สินหรือทะเบียนต่าง ๆ ที่เป็นเอกสารมหาชนหรือที่เป็นข้อมูลสาธารณะ
- ธุรกรรมทางอิเล็กทรอนิกส์ในการให้บริการด้านสาธารณูปโภคและบริการสาธารณะที่ต้องดำเนินการอย่างต่อเนื่องตลอดเวลา

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ประกอบด้วย

(๑) ผลกระทบด้านมูลค่าความเสียหายทางการเงิน

(๒) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรืออนามัย

(๓) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่นใดนอกจาก (๒)

(๔) ผลกระทบด้านความมั่นคงหรือความสงบเรียบร้อยของสังคม

ผลประเมินที่เป็นผลกระทบในระดับ**สูง**ด้านหนึ่งด้านใดให้ธุรกรรมทางอิเล็กทรอนิกส์นั้นต้องใช้วิธีการแบบปลอดภัยระดับ**เคร่งครัด**

ผลกระทบในระดับ**กลาง**อย่างน้อย**สองด้าน**ขึ้นไปให้ใช้วิธีการแบบปลอดภัยในระดับ**กลาง**

ในกรณีที่ไม่เป็นไปตามข้างต้น ให้ธุรกรรมทางอิเล็กทรอนิกส์ใช้วิธีการแบบปลอดภัยในระดับไม่ต่ำกว่าระดับ**พื้นฐาน**

ประกาศนี้ให้ใช้บังคับเมื่อพ้นกำหนด ๓๖๐ วัน นับแต่วันประกาศในราชกิจจานุเบกษา

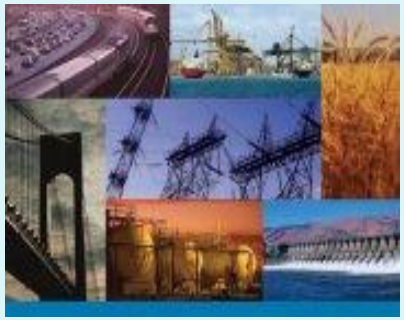
(ร่าง) ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหรือประเภทของหน่วยงานหรือองค์กรหรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ

กลุ่ม ๑
สาธารณูปโภค สาธารสุขและการแพทย์,

กลุ่ม ๒ การผลิต
การพลังงาน
อุตสาหกรรม
ทรัพยากรธรรมชาติ
และสิ่งแวดล้อม

กลุ่ม ๓ ความมั่นคงของประเทศ,

กลุ่ม ๔ ความสงบสุขของสังคมและนันทนาการ



กลุ่ม ๕ การคมนาคม
ขนส่ง และ
สื่อสารมวลชน

กลุ่ม ๖ เทคโนโลยี
สารสนเทศและการ
สื่อสาร

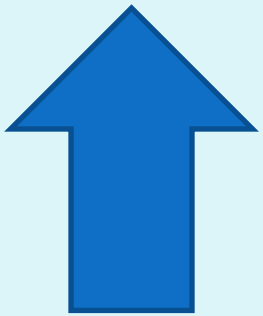
กลุ่ม ๗ การเงิน การค้า
การธนาคาร การลงทุน
และหลักทรัพย์

กลุ่ม ๘ นโยบาย การ
บริหารจัดการภาครัฐ

บทสรุปสำหรับผู้บริหาร

Then……

ยกระดับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ



From now

จัดทำนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ


Thank You