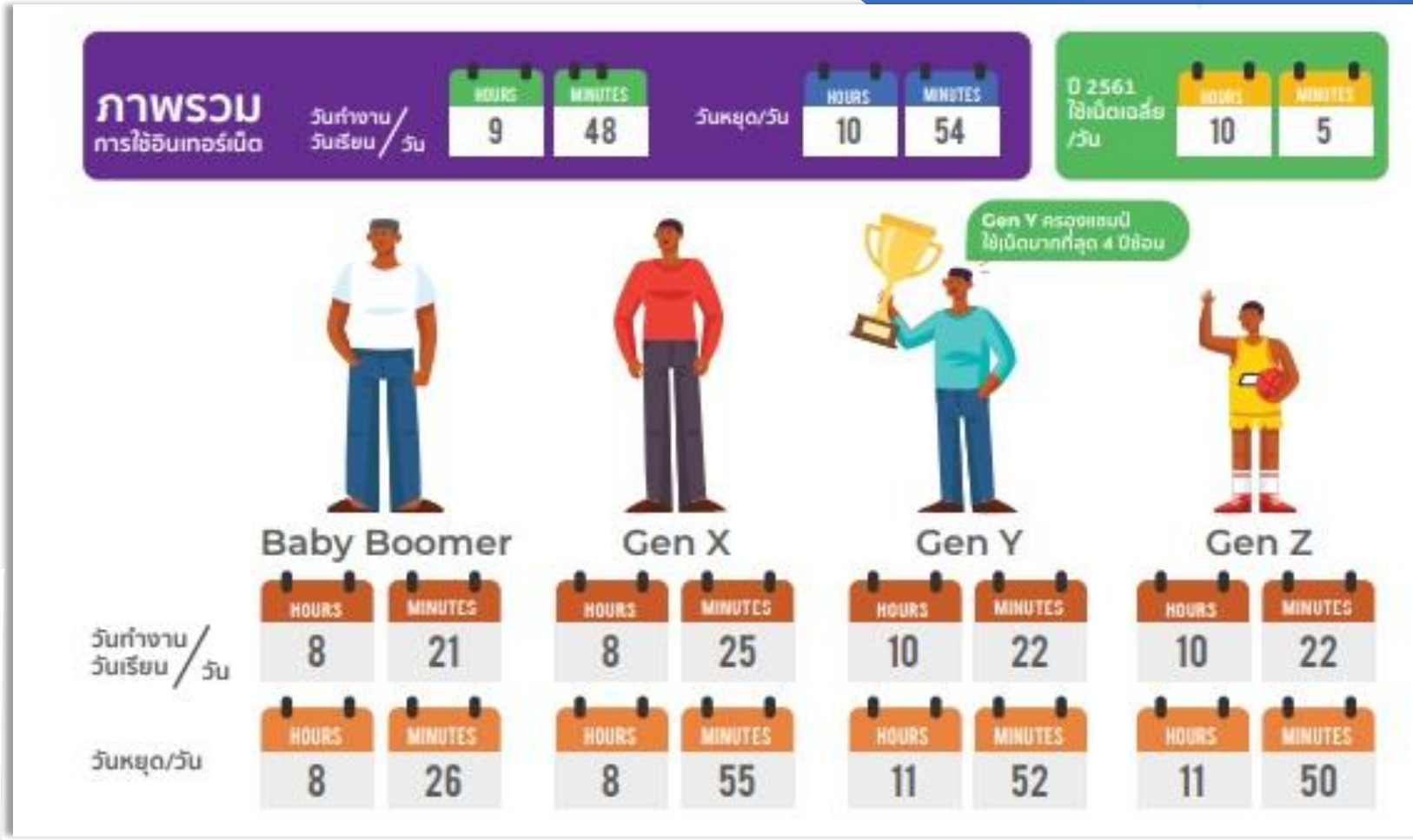
พ.ร.บ. น่ารู้ของคนยุคดิจิทัล 4.0

ณ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

วันศุกร์ที่ 10 พฤษภาคม 2562

1

ทำไมเราถึงต้องรู้เรื่อง พ.ร.บ. ในยุคดิจิทัล



คนไทยใช้อินเทอร์เน็ตทำกิจกรรมมากขึ้น

Source: Thailand Internet User Profile 2018

กิจกรรมยอดฮิต 5 อันดับแรกของคนไทย

Social Media

93.6%

รับ-ส่ง
อีเมล

74.2%

ค้นหาข้อมูล

70.9%

ดูโทรทัศน์
/ฟังเพลง

60.7%

ซื้อสินค้า
และบริการ

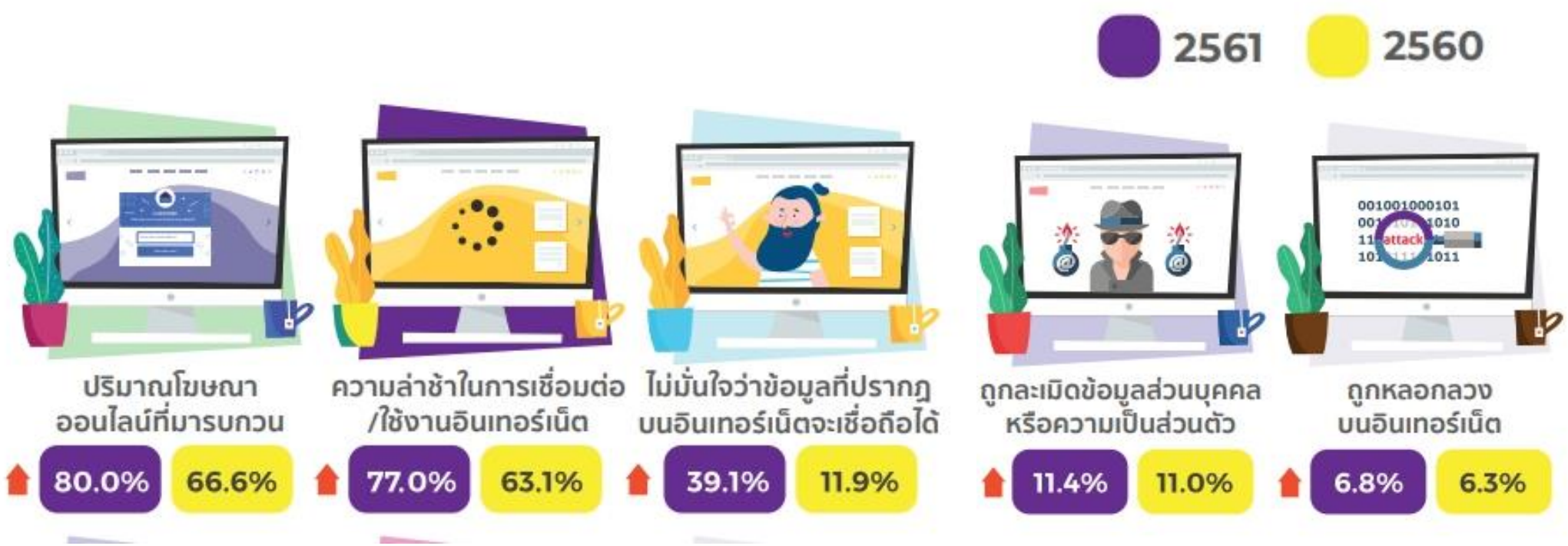
51.3%

	อ่านหนังสือทางออนไลน์	ขายสินค้าและบริการ	จองโรงแรม/ที่พัก	บริการเรียกแท็กซี่	จอง/ซื้อตั๋วยานพาหนะ/การแสดง
ปี 2561	48.3%	24.5%	20.7%	12.6%	21.7%
ปี 2560	30.8%	13.7%	11.0%	4.8%	14.6%

พฤติกรรมการใช้งานกิจกรรมเปลี่ยนแปลงไปใช้บริการต่าง ๆ ทางออนไลน์มากขึ้น

Source: Thailand Internet User Profile 2018

เปรียบเทียบตามปัญหาที่เกิดจากการทำกิจกรรมผ่านอินเทอร์เน็ต ปี 2560 – 2561



Source: Thailand Internet User Profile 2018

มูลค่า e-Commerce

ในประเทศไทย ปี 2560 และคาดการณ์ปี 2561

มูลค่า e-Commerce ปี 2560

2,762,503.22

ล้านบาท

มูลค่า e-Commerce ปี 2561

3,150,232.96

ล้านบาท

อัตราการเติบโต

14.04%

รวม

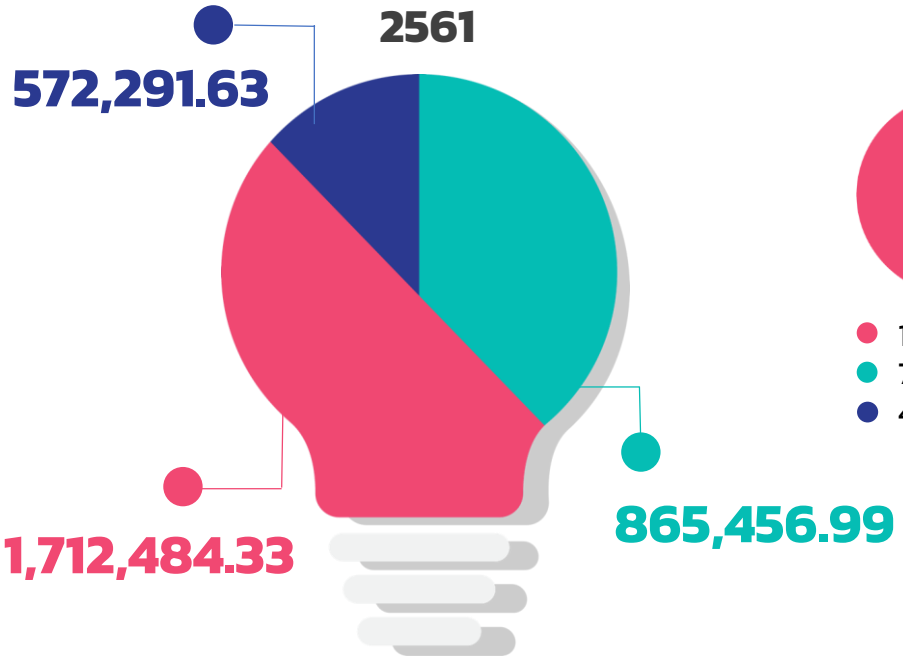
B2B + B2C + B2G

Source: Value of e-Commerce Survey 2561, ETDA

มูลค่า e-Commerce

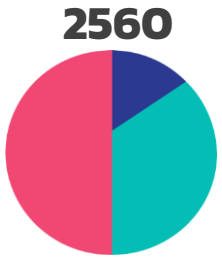
ปี 2558-2560 และคาดการณ์ปี 2561

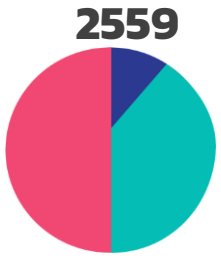
จำแนกตามประเภทผู้ประกอบการ
(รวมมูลค่าการจัดซื้อจัดจ้างของภาครัฐ)

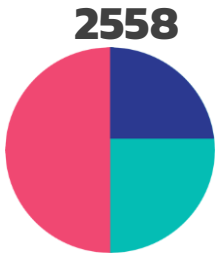


อัตราการเติบโต

- **B2B 13.55%** ธุรกิจเพิ่มช่องทางออนไลน์มากขึ้น
- **B2C 14.04%** พ่อค้าแม่ค้าเข้ามาค้าขายออนไลน์เพิ่มขึ้น
- **B2G 15.50%** e-Gov







Source: Value of e-Commerce Survey 2561, ETDA

หน่วย : ล้านบาท

B2C e-Commerce TOP 5 Ranking in ASEAN

01	TH	$24.70
02	MY	$19.41
03	VN	$8.21
04	SG	$4.61
05	PH	$1.84

หน่วย : พันล้านดอลล่าสหรัฐ

Source: Value of e-Commerce Survey 2561, ETDA

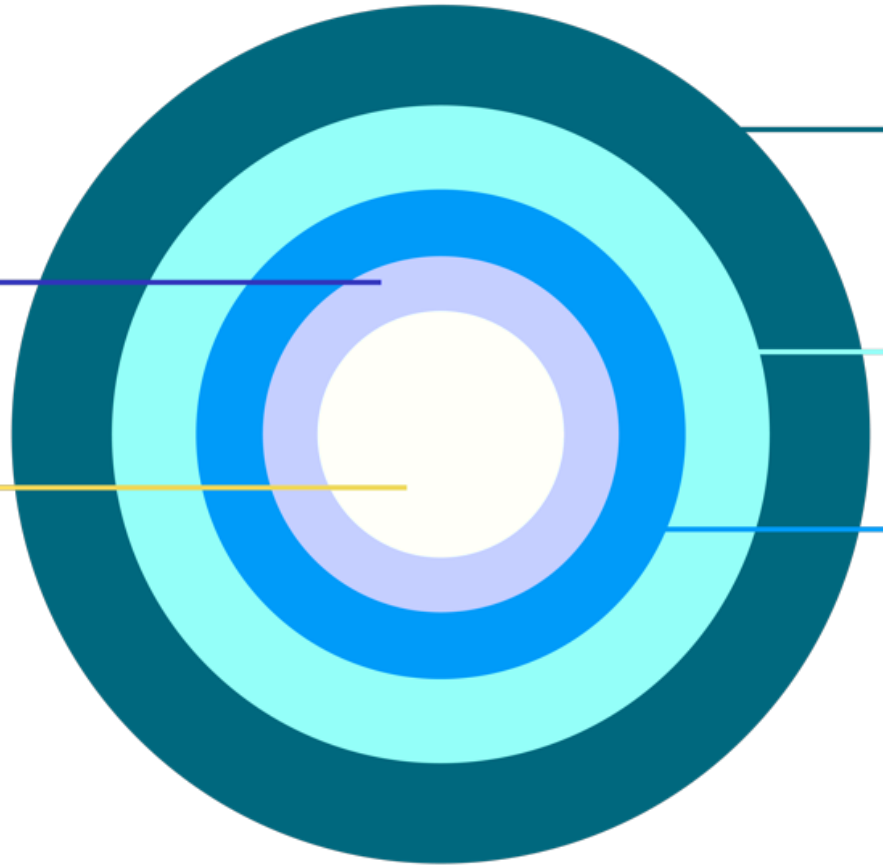
ช่องทางการชำระเงิน
สำหรับธุรกิจ e-Commerce

ยอดนิยม **5** อันดับแรก

ช่องทาง Credit/Debit Card
ผ่าน Payment Gateway
ยังคงได้รับความนิยม

สูงเป็นอันดับ 1

ปัจจัยเสริมคือสถาบันการเงินเร่งส่งเสริมและ
ออกแคมเปญส่งเสริมการขายเชิญชวนให้คนใช้
บัตรมากขึ้น



42.69%
Credit/ Debit Card

27.23%
Internet Banking/
Application

10.75%
Others
- QR Payment
- Purchase Order
- Cheque

10.46%
Banking Counter

7.00%
Cash on Delivery

ที่เหลือ 1.87% เป็นช่องทางอื่น ๆ

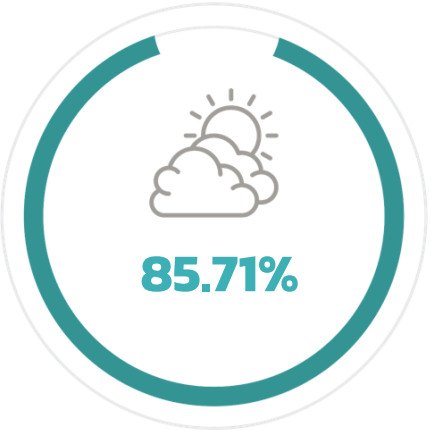
Source: Value of e-Commerce Survey 2561, ETDA

ลักษณะการใช้ข้อมูล Big Data

ของผู้ประกอบการ e-Commerce

วิเคราะห์พฤติกรรมผู้บริโภค
เพื่อนำเสนอสินค้าใหม่ๆ

วิเคราะห์พฤติกรรมผู้บริโภค
เพื่อวางแผนการตลาด



วิเคราะห์ปัจจัยแวดล้อม
เพื่อกำหนดยุทธศาสตร์การจำหน่ายสินค้า

Source: Value of e-Commerce Survey 2561, ETDA

งบประมาณสำหรับการทำ Big Data/Data Analytics

ของผู้ประกอบการ e-Commerce รายใหญ่ในปี 2561 โดยประมาณ

1

46.15%

น้อยกว่า 1 ล้านบาท

2

30.76%

10-50 ล้านบาท

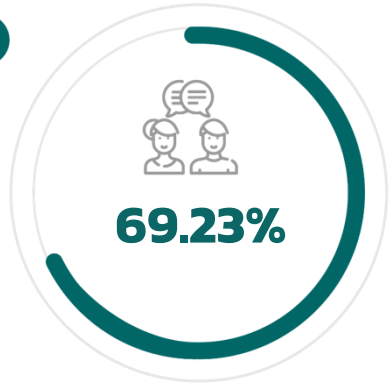
3

23.07%

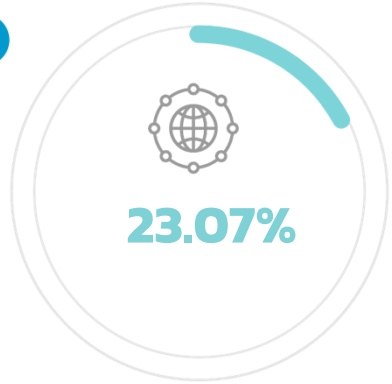
1-5 ล้านบาท

Source: Value of e-Commerce Survey 2561, ETDA

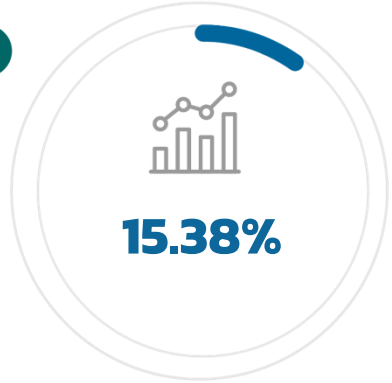
ลักษณะการใช้งาน AI ในการพัฒนาคุณภาพสินค้าและบริการ

1


ช่วยในการให้บริการ
เช่น Chat bot, CRM

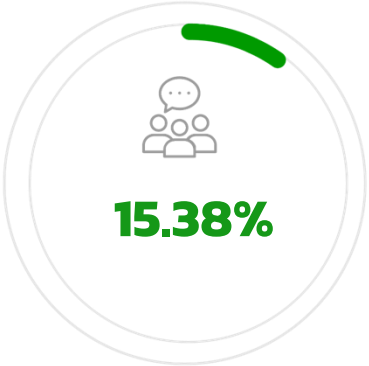
2


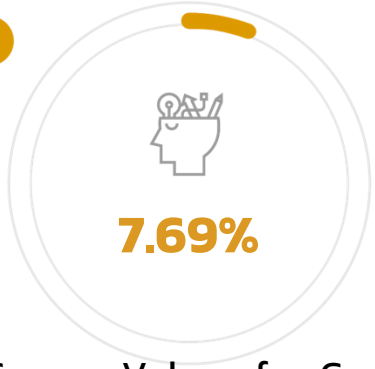
ช่วยในด้านอื่น ๆ
เช่น Claim Analytics, Underwriting, Notification, Daily Operation

3


ช่วยในการวิเคราะห์พฤติกรรมผู้บริโภค
เพื่อพัฒนาการบริการ

ช่วยในการตัดสินใจในเชิงการบริหาร
เช่น การขยายสาขา
การเพิ่ม/ลดพนักงาน
การบริหารภายใน

4


5


ช่วยในด้านการพัฒนาผลิตภัณฑ์
เช่น การออกแบบผลิตภัณฑ์ตัวใหม่

Source: Value of e-Commerce Survey 2561, ETDA

2

ภาพรวม
โครงสร้างกฎหมายด้านดิจิทัล

Digital Law Landscape

PROMOTE & FUNDING	กฎหมายการเพิ่มขีดความสามารถในการแข่งขันของประเทศสำหรับอุตสาหกรรมเป้าหมาย (กองทุนเพิ่มขีดความสามารถในการแข่งขันของประเทศสำหรับอุตสาหกรรมเป้าหมาย)	กฎหมายการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม (กองทุน DE)		ความตกลงระหว่างประเทศ
TRADE FACILITATION	กฎหมายธุรกรรมทางอิเล็กทรอนิกส์	กฎหมายการอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ	ร่างกฎหมายการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล	
DIGITAL INFRASTRUCTURE	กฎหมาย กสทช.	OTT กับแนวทางการดูแลที่เหมาะสม		
DIGITAL PAYMENT	กฎหมายระบบการชำระเงิน	พ.ร.ก. การประกอบธุรกิจสินทรัพย์ดิจิทัล	ร่างประมวลรัษฎากร (จัดเก็บภาษี e-Business)	
SECURE ECOSYSTEM	กฎหมาย Cyber Crime	ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล	ร่างกฎหมาย Cybersecurity	
CONSUMER & BUSINESS TRUST	Online Consumer Protection	Online Disputes Resolution	กฎหมายทรัพย์สินทางปัญญา	กฎหมายความลับทางการค้า	กฎหมายแข่งขันทางการค้า
SOFT LAW	Standard and Self-Regulation			International Standard

สถานะของกฎหมายเศรษฐกิจดิจิทัล (ที่อยู่ระหว่างกระบวนการเสนอกฎหมาย)

๑. กฎหมายธุรกรรมทางอิเล็กทรอนิกส์

๑.๑ (ร่าง) พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ..) พ.ศ. .... • ปรับปรุงหลักเกณฑ์ e-transaction ให้สอดคล้องตามหลักสากล	มีผลใช้บังคับแล้ว
๑.๒ (ร่าง) พ.รบ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ..) พ.ศ. .... • เพิ่มเติมบทบัญญัติเรื่องระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล (Digital ID)	สนช. เห็นสมควรประกาศใช้เป็นกฎหมาย (อยู่ระหว่างการนำขึ้นทูลเกล้าฯ)
๒. (ร่าง) พ.ร.บ.สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.	มีผลใช้บังคับแล้ว
๓. (ร่าง) พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.	สนช. เห็นสมควรประกาศใช้เป็นกฎหมาย (อยู่ระหว่างการนำขึ้นทูลเกล้าฯ)
๔. (ร่าง) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.	สนช. เห็นสมควรประกาศใช้เป็นกฎหมาย (อยู่ระหว่างการนำขึ้นทูลเกล้าฯ)
๕. (ร่าง) พ.ร.บ.การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.	สนช. เห็นสมควรประกาศใช้เป็นกฎหมาย (อยู่ระหว่างการนำขึ้นทูลเกล้าฯ)
๖. (ร่าง) พ.ร.บ.สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย พ.ศ.	มีผลใช้บังคับแล้ว

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ธุรกรรมทางอิเล็กทรอนิกส์ คือ?

ธุรกรรมที่กระทำขึ้นโดย “ใช้วิธีการทางอิเล็กทรอนิกส์” ทั้งหมดหรือแต่บางส่วน

พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ฯ → **เสริม** → **ประมวลกฎหมายแพ่งและพาณิชย์**

ตัวอย่าง ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 456

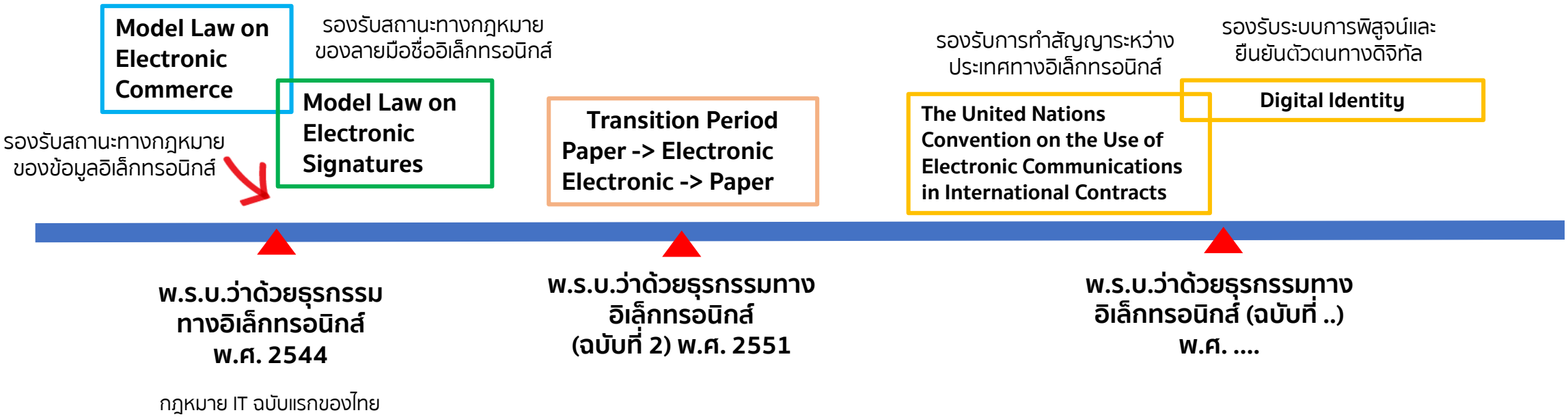
สัญญาซื้อขาย
สังหาริมทรัพย์
ราคาตั้งแต่ **20,000 บาท** → e-Document ม. 8
ต้องมี**หลักฐานเป็นหนังสือ**
ลงลายมือชื่อฝ่ายที่ต้องรับ → e-Signature ม.9
ผิดเป็นสำคัญ

หมายเหตุ กฎหมายธุรกรรมทางอิเล็กทรอนิกส์**ไม่ใช้**กับ

(1) ธุรกรรมเกี่ยวกับครอบครัว

(2) ธุรกรรมเกี่ยวกับมรดก

พัฒนาการกฎหมายธุรกรรมทางอิเล็กทรอนิกส์ของไทย



Online Dispute Resolution
การระงับข้อพิพาททางออนไลน์

Electronic Transferable Records
เอกสารเปลี่ยนมือได้ในรูปแบบข้อมูลอิเล็กทรอนิกส์

Identity Management and Trust Services
การจัดการการระบุตัวตนทางอิเล็กทรอนิกส์ และบริการที่เชื่อถือได้

การพัฒนาที่ต่อเนื่อง

UNCITRAL Model Law on
Electronic Commerce

Legislation based on or influenced by the Model Law has been adopted in 71 States

UNCITRAL Model Law on
Electronic Signatures

Legislation based on or influenced by the Model Law has been adopted in 32 States

กฎหมายที่โยงมายังกฎหมายธุรกรรมทางอิเล็กทรอนิกส์

- พ.ร.บ. ศุลากร พ.ศ. 2560

มาตรา ๑๑ การดำเนินการทางศุลากร ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ ให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกันกับการดำเนินการทางศุลกากรโดยเอกสาร ทั้งนี้ การนำข้อมูลอิเล็กทรอนิกส์มาใช้ในการศุลกากรให้เป็นไปตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

- พ.ร.บ. ปปช. พ.ศ. 2561

มาตรา ๑๐๕ วรรคสอง
หลักเกณฑ์ ระยะเวลา การขยายระยะเวลา วิธีการยื่นบัญชีทรัพย์สินและหนี้สิน และหลักฐานประกอบตามวรรคหนึ่งให้เป็นไปตามที่คณะกรรมการ ป.ป.ช. กำหนด โดยอาจกำหนดให้ยื่นด้วยวิธีการทางอิเล็กทรอนิกส์ก็ได้ การกำหนดดังกล่าวให้คำนึงถึงวิวัฒนาการของเทคโนโลยีที่เหมาะสมกับรูปแบบและวิธีการใช้อิเล็กทรอนิกส์แทนการใช้เอกสารได้ด้วย รวมทั้งให้สอดคล้องกับกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ระยะเวลาที่กำหนดให้ยื่นบัญชีทรัพย์สินและหนี้สินดังกล่าวต้องไม่น้อยกว่าหกสิบวัน

- "ข้อบังคับสถาบันอนุญาโตตุลาการ ว่าด้วยการระงับข้อพิพาทด้วยวิธีการทางอิเล็กทรอนิกส์สำหรับธุรกรรมพาณิชย์อิเล็กทรอนิกส์ พ.ศ. ๒๕๕๘"

ข้อ ๔ การระงับข้อพิพาทด้วยวิธีการทางอิเล็กทรอนิกส์สำหรับธุรกรรมพาณิชย์อิเล็กทรอนิกส์ให้เป็นไปตามข้อบังคับนี้ ในกรณีที่ไม่มีข้อบทใดในข้อบังคับนี้ ให้นำกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์มาใช้บังคับโดยอนุโลม

- "ระเบียบกรมพัฒนาธุรกิจการค้า ว่าด้วยหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๗"

ข้อ ๙ การจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ ต้องเป็นไปตามข้อกำหนดแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์ และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ ฉบับที่ ๑ ว่าด้วยข้อกำหนดวิธีปฏิบัติในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์

- "ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์สำหรับการนำเข้า การส่งออก การนำผ่าน และโลจิสติกส์ พ.ศ. ๒๕๕๗"

ข้อ ๓ นอกจากที่บัญญัติไว้ในระเบียบนี้ ในการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ ให้หน่วยงานของรัฐดำเนินการและปฏิบัติตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

- "ประกาศสำนักงานคณะกรรมการส่งเสริมการลงทุน ที่ ป. ๒/๒๕๕๔ เรื่อง วิธีปฏิบัติในการใช้สิทธิประโยชน์สำหรับเครื่องจักรด้วยระบบอิเล็กทรอนิกส์แบบครบวงจร"

๒. การดำเนินการในทางปฏิบัติอื่นใดเกี่ยวกับการรับคำขอ และการใช้สิทธิประโยชน์ด้านเครื่องจักรผ่านเครือข่ายอินเทอร์เน็ต ที่มิได้กำหนดไว้ตามประกาศนี้ ให้ถือปฏิบัติตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

ตัวอย่างหน่วยงานรัฐที่เปลี่ยนระบบจากกระดาษเป็นอิเล็กทรอนิกส์

1. เนติบัณฑิตยสภา
   - (ระบบให้บริการออกหนังสือรับรองทางอิเล็กทรอนิกส์ (e-Certificate))

2. กรมพัฒนาธุรกิจการค้า
   - (การให้บริการหนังสือรับรองนิติบุคคลทางอิเล็กทรอนิกส์)

3. มหาวิทยาลัยขอนแก่น
   - (การจัดเก็บเอกสารสัญญากู้ยืมเงินเพื่อการศึกษาด้วยระบบอิเล็กทรอนิกส์)

4. สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
   - (e-Insurance)

5. กรมสรรพากร
   - (การจัดทำ ส่งมอบ และเก็บรักษาใบกำกับภาษีอิเล็กทรอนิกส์ด้วยระบบการจัดทำและส่งใบกำกับภาษีอิเล็กทรอนิกส์ผ่านระบบ e-Tax Invoice by Email)

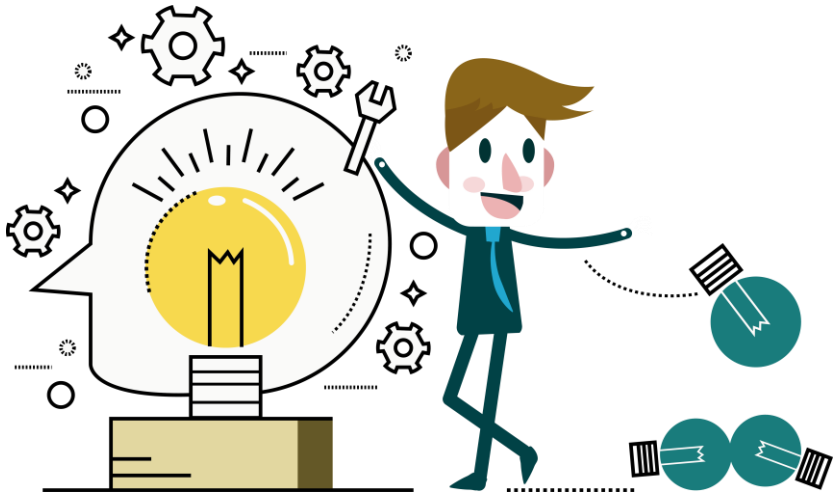
กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

หลักการสำคัญของกฎหมายธุรกรรมฯ

“รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์” (ม.7)

Non-Discrimination

รองรับให้ธุรกรรมกระดาษตามที่กฎหมายกำหนด ทำในรูปแบบข้อมูลอิเล็กทรอนิกส์ได้



- หลักความเท่าเทียมกัน
  Functional Equivalent Approach
- หลักความเป็นกลางทางเทคโนโลยี
  Technology Neutrality
- หลักเสรีภาพในการแสดงเจตนา
  Party Autonomy

โครงสร้างกฎหมาย

- **“ธุรกรรมทางอิเล็กทรอนิกส์”**
  รองรับการทำธุรกรรมในรูปแบบข้อมูลอิเล็กทรอนิกส์ในเรื่องต่าง ๆ

- **“ลายมือชื่ออิเล็กทรอนิกส์”**
  รองรับลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

- **“ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์”**
  รองรับการกากับดูแลธุรกิจบริการที่เกี่ยวข้องกับการทาธุรกรรมทางอิเล็กทรอนิกส์ที่สำคัญ และมีผลกระทบวงกว้าง

- **“ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ”**
  รองรับการให้บริการภาครัฐด้วยวิธีการทางอิเล็กทรอนิกส์

- **“คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์”**
  รองรับการมีคณะกรรมการเพื่อส่งเสริมและพัฒนาการทาธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ

Mandatory Rules

เมื่อตกลงใช้ธุรกรรมอิเล็กทรอนิกส์
หลักเกณฑ์เหล่านี้จะตกลงเป็นอย่างอื่นไม่ได้

- ม.7 ห้ามปฏิเสธเพียงเพราะเป็นธุรกรรมที่ทำในแบบอิเล็กทรอนิกส์
- ม.8 การทำข้อมูลอิเล็กทรอนิกส์เป็นหนังสือ
- ม.9 การลงลายมือชื่อในข้อมูลอิเล็กทรอนิกส์
- ม.10 ความเป็นต้นฉบับของข้อมูลอิเล็กทรอนิกส์
- ม.11 การรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานในศาล
- ม.12 การเก็บรักษาข้อมูลอิเล็กทรอนิกส์
- ม.12/1 การแปลงเอกสารกระดาษเป็นข้อมูลิเล็กทรอนิกส์
- ม. 25 วิธีการที่เชื่อถือได้ที่ได้ประโยชน์จากข้อสันนิษฐานทางกฎหมาย

หลักเกณฑ์อื่นนอกจากนี้ในหมวด 1 และ 2 สามารถตกลงเป็นอย่างอื่นได้

3

หลักการสำคัญของกฎหมายธุรกรรมฯ

กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ กับ วงจรเอกสาร

e-Document (ม.8)

e-Signature

ความเป็นต้นฉบับของข้อมูลอิเล็กทรอนิกส์ (ม.10)

(ม.9)
ลายมือชืออิเล็กทรอนิกส์แบบทั่วไป
เช่น Username Password

(ม. 26)
ลายมือชืออิเล็กทรอนิกส์ที่เชื่อถือได้
เช่น PKI

การเก็บรักษาข้อมูลอิเล็กทรอนิกส์ (ม.12)

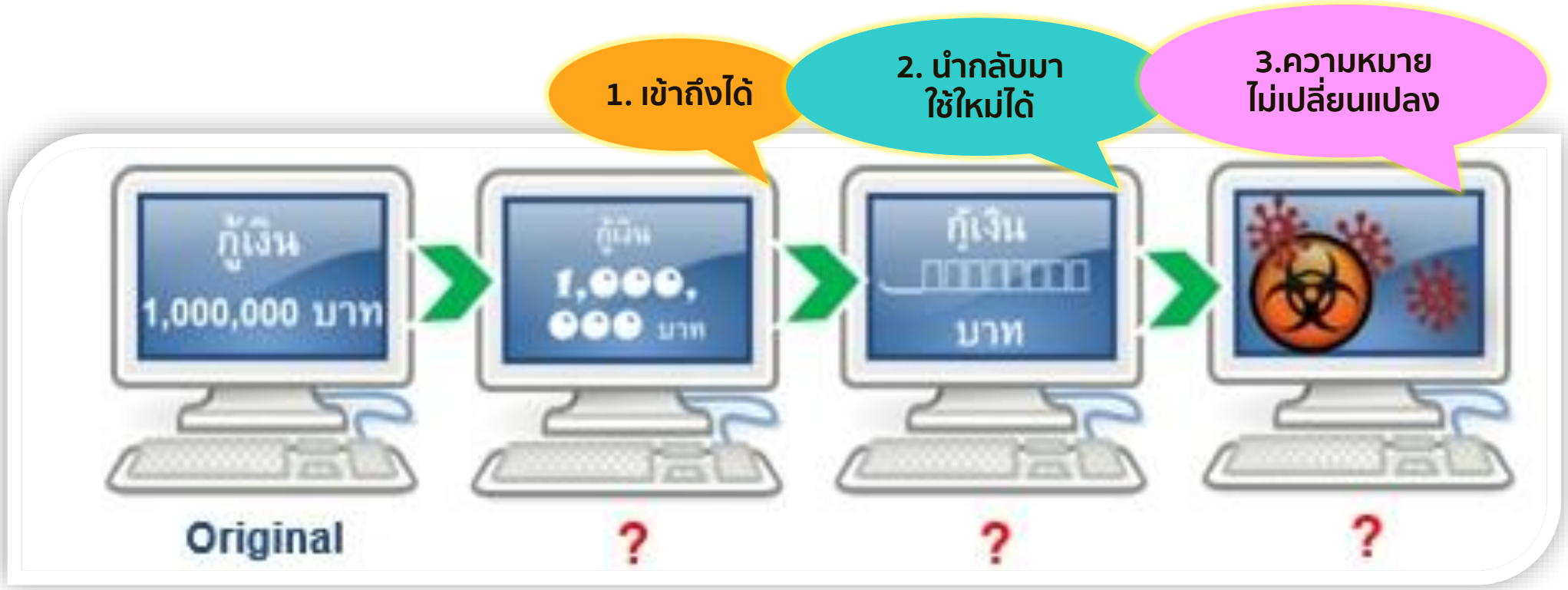
การแปลงเอกสาร
(ม.12/1)

การรับรองสิ่งพิมพ์ออก
(ม.10 วรรค4)

Transition Period

1.

E-document



หากเป็นไปตามเงื่อนไขครบทั้ง 3 ข้อ
ให้ถือว่า ข้อความนั้นได้ทำเป็นหนังสือหรือมีหลักฐานเป็นหนังสือแล้ว

2.

หลักการของ“ลายมือชื่ออิเล็กทรอนิกส์”

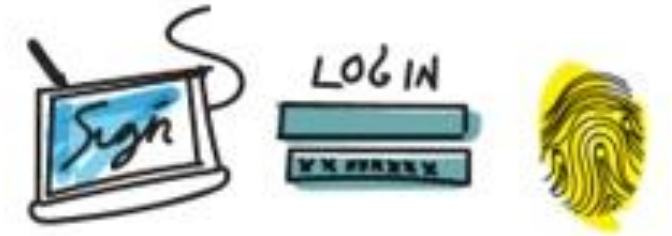
สิ่งที่ใช้เชื่อมโยงเพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ และ เพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในรูปข้อมูลอิเล็กทรอนิกส์

PKI

E-Signature ม.9

หลักการสำคัญ

1. ระบุตัวผู้เป็นเจ้าของลายมือชื่อได้
2. แสดงได้ว่าเจ้าของลายมือชื่อยอมรับข้อความนั้น
3. ใช้วิธีการที่น่าเชื่อถือ



- ความมั่นคงและรัดกุมของวิธีการที่จะใช้
- ลักษณะหรือประเภทของขนาดธุรกรรมที่ทำ
- ความรัดกุมของระบบติดต่อสื่อสาร

หากเป็นไปตามเงื่อนไขที่กฎหมายกำหนด ให้ถือว่า มีการลงลายมือชื่อแล้ว

หลัก e-Signature และลายมือชื่อที่เชื่อถือได้ (ม.9+26)

ม. 9

1. ระบุตัวผู้เป็นเจ้าของลายมือชื่อได้
2. แสดงได้ว่าเจ้าของลายมือชื่อยอมรับข้อความนั้น
3. ใช้วิธีการที่น่าเชื่อถือ

ม. 26

ลายมือชื่อที่เชื่อถือได้

1. ข้อมูลที่ใช้สร้างลายมือชื่อเชื่อมโยงไปยังเจ้าของได้
2. ข้อมูลที่ใช้สร้างลายมือชื่ออยู่ภายใต้การควบคุมของเจ้าของ เมื่อสร้าง
3. สามารถตรวจพบการเปลี่ยนแปลงของลายมือชื่อ / ข้อความ นับแต่สร้างได้

ข้อกำหนดของประธานศาลฎีกา ว่าด้วยการยื่น ส่ง และรับคำคู่ความและเอกสารทางระบบรับส่งอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๐

กรณีคู่ความหรือทนายความใช้กลไกการยืนยันตัวตนและการระบุตัวตนแบบ User Name และ Password โดยให้ถือว่ามีการลงลายมือชื่อ

(ข้อ ๕ และข้อ ๙)

ข้อ ๕ เมื่อผู้ยื่นคำขอใช้ระบบรับส่งอิเล็กทรอนิกส์ได้รับอนุญาตให้เป็นผู้ใช้ระบบตามเงื่อนไขและวิธีการที่กำหนดไว้ในประกาศสำนักงานศาลยุติธรรมแล้ว จะได้รับชื่อผู้ใช้ระบบและรหัสผ่าน เพื่อใช้เข้าสู่ระบบรับส่งอิเล็กทรอนิกส์

ชื่อผู้ใช้ระบบและรหัสผ่านเป็นหลักฐานแสดงการลงลายมือชื่อของผู้ใช้ระบบในการติดต่อกับศาลหรือคู่ความอื่นผ่านระบบรับส่งอิเล็กทรอนิกส์ ผู้ใช้ระบบต้องเก็บรักษาชื่อผู้ใช้ระบบและรหัสผ่านไว้เป็นความลับ การระบุชื่อผู้ใช้ระบบและรหัสผ่านลงในระบบรับส่งอิเล็กทรอนิกส์เพื่อเข้าใช้ระบบตามข้อกำหนดนี้ ถือเป็นการยืนยันตัวผู้ใช้ระบบและการรับรองข้อความในข้อมูลอิเล็กทรอนิกส์

ยกตัวอย่างการทำกิจกรรมในมหาวิทยาลัย ที่สอดคล้องกับหลักการฯ

USER ACCOUNT หรือระบบอีเมลของมหาวิทยาลัย

- การลงทะเบียนขอใช้ระบบ ถือเป็น **การเชื่อมโยง** ผู้ใช้ กับ User Account และ Password ที่ได้รับมา
- เมื่อผู้ใช้ทำการ log in (โดยใช้ User Account และ Password) ระบบจะสามารถระบุได้ว่า **ใครทำการยืนยันตัวตนเข้ามาสู่ระบบ**
  *ข้อสังเกต User Account และ Password เป็นความลับ ควรมีเพียงเจ้าของเท่านั้นที่ทราบ (หากไม่นับรวมไปถึงระบบ)
- การทำธุรกรรมต่าง ๆ ภายหลังจากการ log in เข้าสู่ระบบ เช่น การลงทะเบียนวิชาเรียนของนักศึกษา การเบิกเงินสวัสดิการของบุคลากร **ถือได้ว่า เป็นการกระทำของผู้ใช้ ซึ่งได้มีการลงลายมือชื่อและรับรองการทำธุรกรรมนั้นแล้ว**

http://icit.kmutnb.ac.th/main/introduce-icit-account/
http://icit.kmutnb.ac.th/main/services/

3.

รองรับ e-EVIDENCE เพื่อใช้เป็นหลักฐานในการดำเนินคดี

ม. 11 ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในศาล

แต่ การที่ศาลจะเชื่อถือในพยานหลักฐานอิเล็กทรอนิกส์หรือไม่ ขึ้นอยู่กับ

- ✓ ความน่าเชื่อถือของพยานหลักฐาน
- ✓ การชั่งน้ำหนักพยานหลักฐานของศาลเอง

ความน่าเชื่อถือของพยานหลักฐานพิจารณาจาก

- ลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์
- ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วนและไม่มีการเปลี่ยนแปลง
- ลักษณะ วิธีการที่ใช้ในการระบุตัวผู้ส่งข้อมูล
- พฤติการณ์ที่เกี่ยวข้องทั้งปวง

จะลดความเสี่ยง และ เพิ่มความน่าเชื่อถือ ได้อย่างไร

1 สอดคล้องกับมาตรฐานขั้นต่ำที่กฎหมายกำหนด

เช่น หลักเกณฑ์/องค์ประกอบ ตาม ม.8 ถึง ม. 24 และ ม.26 ถึง ม. 31

มาตรฐานการแปลงเอกสาร (ม.12/1)

มาตรฐานของวิธีแบบปลอดภัย (ม.25) ที่ได้ประโยชน์จากข้อสันนิษฐานทางกฎหมาย ว่าได้ใช้วิธีการที่เชื่อถือได้

2. แนวทางการชั่งน้ำหนักพยานหลักฐาน (ม.๑๑)

พิจารณาจาก

- ลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์
- ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วนและไม่มีการเปลี่ยนแปลง
- ลักษณะ วิธีการที่ใช้ในการระบุตัวผู้ส่งข้อมูล
- พฤติการณ์ที่เกี่ยวข้องทั้งปวง

3. มาตรฐาน

- มาตรฐานสากลต่างๆ
- มาตรฐาน คธอ.
- มาตรฐาน สพธอ.

คำพิพากษาไทย (8089/2556)

- การเบิกถอนเงินสดจากบัญชีสินเชื่อเงินสด ผ่านตู้ ATM เป็นธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งรับฟังได้ตามมาตรา 7
- การนำบัตรกดเงินสดไปถอดนงินและใส่รหัสส่วนตัว เสมือนการลงลายมือชื่อตนเอง ซึ่งถือเป็นการลงลายมือชื่ออิเล็กทรอนิกส์ตามมาตรา 9
- เมื่อจำเลยนำบัตรกดเงินสดไปถอนเงิน ใส่รหัสเพื่อทำรายการถอนเงิน และกดยืนยันทำรายการ พร้อมรับเงินสดและสลิป การกระทำดังกล่าวจึงถือเป็นหลักฐานการกู้ยืมเงิน ตามมาตรา 8 วรรค 1

คำพิพากษาไทย (6757/2560)

- การส่งข้อความผ่าน Facebook เพื่อยกหนี้ให้ ถือเป็นการส่งข้อมูลอิเล็กทรอนิกส์ ตาม ม.7 กฎหมายธุรกรรมทางอิเล็กทรอนิกส์
- และถือว่าได้มีการทำเป็นหนังสือ หรือมีหลักฐานเป็นหนังสือแล้วตาม ม. 8 กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
- รวมทั้งเมื่อปรากฏว่าการส่งข้อความดังกล่าวมีชื่อผู้ส่งด้วย จึงถือว่า ได้มีการลงลายมือชื่อตาม ม. 9 กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

e-Court

พ.ร.บ. แก้ไขเพิ่มเติมประมวลวิธีพิจารณาความแพ่ง (ฉบับที่ 28) พ.ศ. 2558

ประกาศราชกิจจานุเบกษาเมื่อ 8 ตุลาคม 2558

- ✓ **รองรับการจัดทำสารบบความ สำนวนความ ในรูปแบบข้อมูลอิเล็กทรอนิกส์ รวมถึง Print out ของข้อมูลดังกล่าว**
- ✓ **รองรับการยื่นคำคู่ความและเอกสารใน รูปแบบข้อมูลอิเล็กทรอนิกส์ เช่น การยื่น ผ่านทางอีเมล**

การจัดทำสารบบความสำนวนความในรูปแบบข้อมูลอิเล็กทรอนิกส์

มาตรา ๗ ให้เพิ่มความต่อไปนี้เป็นวรรคสองของมาตรา ๕๑ แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง

“การจัดทำสารบบความหรือสารบบคำพิพากษา การรวบรวมเอกสารในสำนวนความ และการเก็บรักษาสำเนาคำพิพากษาหรือคำสั่งชี้ขาดคดีตามวรรคหนึ่ง (๑) (๒) (๓) (๔) และ (๕) อาจกระทำในรูปแบบข้อมูลอิเล็กทรอนิกส์ก็ได้ และให้ถือว่าสิ่งพิมพ์ออกของข้อมูลอิเล็กทรอนิกส์ดังกล่าวที่รับรองโดยวิธีการที่ศาลกำหนดเป็นสำเนาสารบบความหรือสารบบคำพิพากษา หรือเป็นสำเนาเอกสารในสำนวนความแล้วแต่กรณี และให้ใช้แทนต้นฉบับได้ ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่กำหนดไว้ในข้อกำหนดของประธานศาลฎีกาโดยความเห็นชอบของที่ประชุมใหญ่ศาลฎีกา และเมื่อข้อกำหนดนั้นประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้”

การยื่นคำคู่ความ และเอกสารในรูปแบบข้อมูลอิเล็กทรอนิกส์

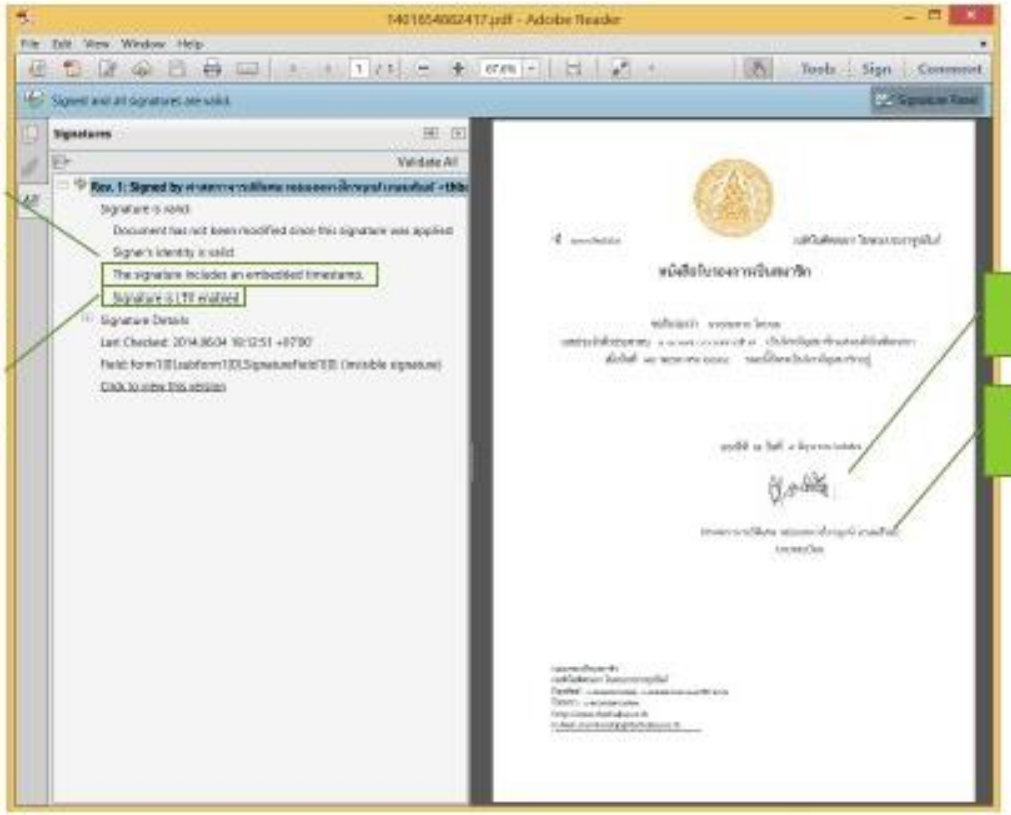
มาตรา ๙ ให้ยกเลิกความในมาตรา ๖๘ แห่งประมวลกฎหมายวิธีพิจารณาความแพ่งและให้ใช้ความต่อไปนี้แทน

“มาตรา ๖๘ การยื่นและส่งคำคู่ความและเอกสารในลักษณะนี้ไม่ว่าการนั้นจะเป็นโดยคู่ความฝ่ายใดทำต่อศาลหรือต่อคู่ความอีกฝ่ายหนึ่ง หรือศาลทำต่อคู่ความฝ่ายใดฝ่ายหนึ่ง หรือทุกฝ่าย รวมทั้งการแจ้งคำสั่งของศาลหรือข้อความอย่างอื่นไปยังคู่ความหรือบุคคลอื่นใด อาจดำเนินการโดยทางไปรษณีย์อิเล็กทรอนิกส์หรือสื่อเทคโนโลยีสารสนเทศอื่นใดก็ได้ ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่กำหนดไว้ในข้อกำหนดของประธานศาลฎีกาโดยความเห็นชอบของที่ประชุมใหญ่ศาลฎีกา และเมื่อข้อกำหนดนั้นประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้”

ระบบให้บริการออกหนังสือรับรองทางอิเล็กทรอนิกส์ (e-Certificate)

มีประทับรับรองเวลา (Time Stamping) ร่วมกับ Digital Signature

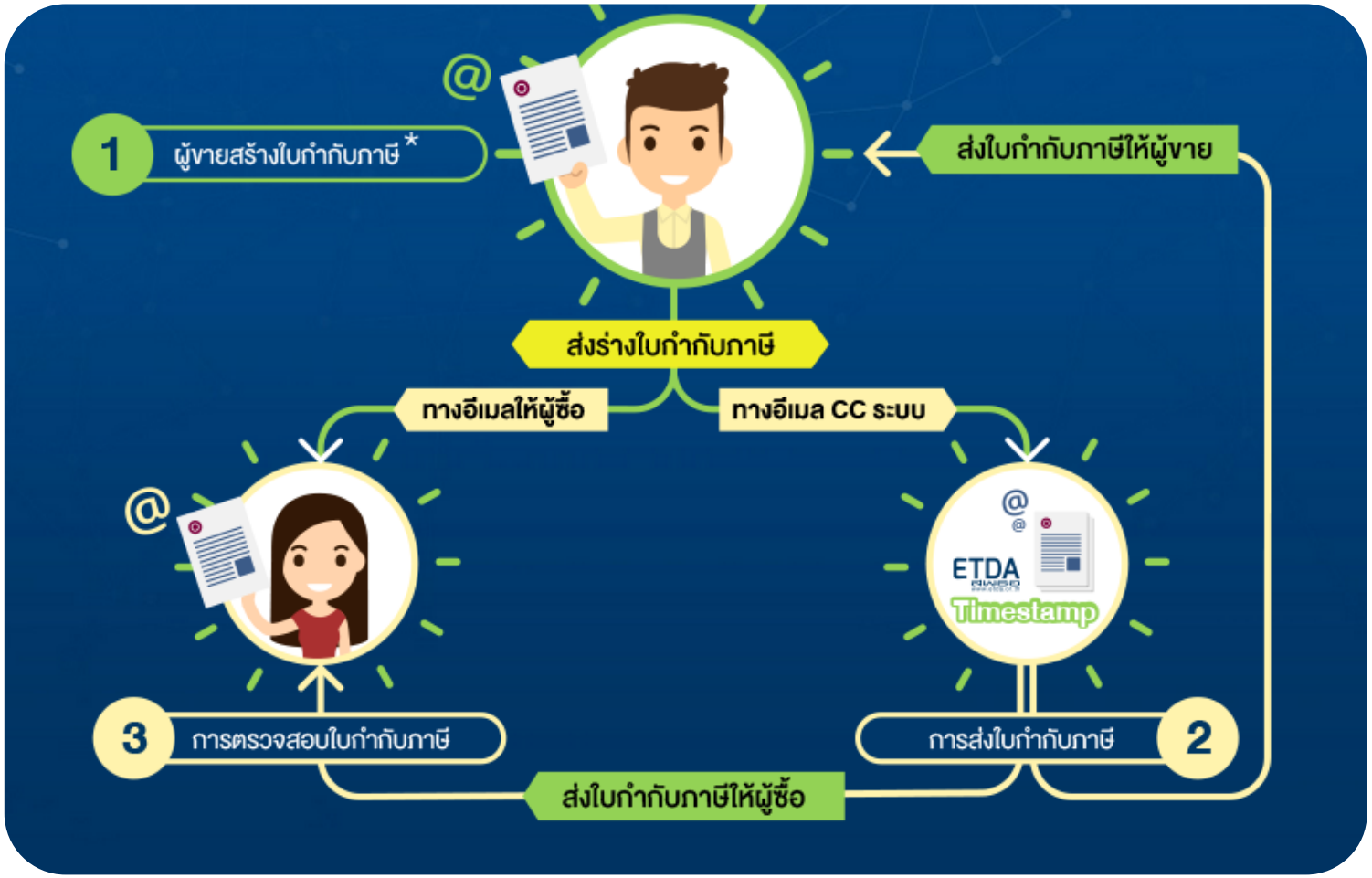
มีการรวม Certificate Chain และ CRL เพื่อรองรับ Long-Term Validation ตามมาตรฐาน PAdES



แสดงภาพลายเซ็นมีย Digital Signature นั้น Valid

แสดงชื่อ-สกุล และตำแหน่งภาษาไทย โดยดึงค่าจาก Certificate

e-Tax Invoice by E-mail



4.

วิธีการแบบปลอดภัยสำคัญอย่างไร

ประโยชน์จาก **ข้อสันนิษฐานตามกฎหมาย**
ว่าได้ใช้ **วิธีการที่น่าเชื่อถือ** ในการทำธุรกรรม

มาตรา ๒๔ ธุรกรรมทางอิเล็กทรอนิกส์ที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็นวิธีการที่เชื่อถือได้

วิธีการที่เชื่อถือได้

มาตรา ๙ ในกรณีที่บุคคลพึงลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้า

(๑) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ

(๒) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

วิธีการที่เชื่อถือได้ตาม (๒) ให้คำนึงถึง

ก. ความมั่นคงและรัดกุมของการใช้วิธีการหรืออุปกรณ์ในการระบุตัวบุคคล สภาพพร้อมใช้งานของทางเลือกในการระบุตัวบุคคล กฎเกณฑ์เกี่ยวกับลายมือชื่อที่กำหนดไว้ในกฎหมายระดับความมั่นคงปลอดภัยของการใช้ลายมือชื่ออิเล็กทรอนิกส์ การปฏิบัติตามกระบวนการในการระบุตัวบุคคลผู้เป็นสื่อกลาง ระดับของการยอมรับหรือไม่ยอมรับ วิธีการที่ใช้ในการระบุตัวบุคคลในการทำธุรกรรม วิธีการระบุตัวบุคคล ณ ช่วงเวลาที่มีการทำธุรกรรมและติดต่อสื่อสาร

ข. ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำ จำนวนครั้งหรือความสม่ำเสมอในการทำธุรกรรม ประเพณีทางการค้าหรือทางปฏิบัติ ความสำคัญ มูลค่าของธุรกรรมที่ทำ หรือ

ค. ความรัดกุมของระบบการติดต่อสื่อสาร

ให้นำความในวรรคหนึ่งมาใช้บังคับกับการประทับตราของนิติบุคคลด้วยวิธีการทางอิเล็กทรอนิกส์ ด้วยโดยอนุโลม

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

มาตรา 25 วิธีการแบบปลอดภัย

พ.ร.ฎ.วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ฯ

ประกาศ คธอ. เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555

- เกณฑ์การประเมินผลกระทบ
- ประเภทธุรกรรมฯ แบบเคร่งครัด

ประกาศ คธอ. เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555

- ระดับเคร่งครัด
- ระดับกลาง
- ระดับพื้นฐาน

ประกาศ คธอ. เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559

ที่มา คธอ.

5.

การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

พ.ร.บ. การจัดซื้อจัดจ้างและบริหารพัสดุภาครัฐ พ.ศ. 2560

กำหนดคำนิยามคำว่า หน่วยงานของรัฐ” ไว้ในมาตรา 4 ดังนี้

“หน่วยงานของรัฐ” หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณ องค์การมหาชน องค์กรอิสระ องค์กรตามรัฐธรรมนูญ หน่วยธุรการของศาล **“มหาวิทยาลัยในกำกับของรัฐ”** หน่วยงานสังกัดรัฐสภาหรือในกำกับของรัฐสภา หน่วยงานอิสระของรัฐ และหน่วยงานอื่นตามที่กำหนดในกฎกระทรวง

พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

มาตรา 35 คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใด ๆ ตามกฎหมายกับ **หน่วยงานของรัฐ** หรือ **โดยหน่วยงานของรัฐ** ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ ตาม**หลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกา** ให้นำพระราชบัญญัตินี้มาใช้บังคับและ **ให้ถือว่ามีผลโดยชอบด้วยกฎหมาย** เช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด

พ.ร.ฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

มาตรา 7 กำหนดให้มีหน้าที่ต้องออกประกาศ “แนวนโยบายและแนวปฏิบัติ” 2 เรื่อง (มตามประกาศ คธอ.

- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและ**แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ**ของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและ**แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล**ของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ภาพรวมกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562

1. ปรับปรุงหลักเกณฑ์ที่มีอยู่เดิม

คำนิยาม (มาตรา 5)

e-Document (มาตรา 8),

e-Signature (มาตรา 9 และมาตรา 26 (4)),

เกณฑ์การส่งข้อมูล (มาตรา 16)

e-Government (มาตรา 35)

2. Harmonize Law with UN E-Communication Convention

- **Invitations to make offers**
  (การเชื้อเชิญเพื่อทำคำเสนอ มาตรา 13/1)
- **Automatic Data System**
  (การทำสัญญาผ่านระบบข้อมูลอัตโนมัติ มาตรา 13/2)
- **Input Error** (การลงข้อมูลผิดพลาด มาตรา 17/1)

3. ปรับปรุงกลไกการดูแลธุรกิจบริการและบทกำหนดโทษ

(มาตรา 32 – มาตรา 34/2, มาตรา 44 – มาตรา 45)

4. ปรับองค์ประกอบและอำนาจหน้าที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

(มาตรา 36 – มาตรา 41 และมาตรา 43/1)

5. จัดตั้งหน่วยงานเพื่อส่งเสริมธุรกรรมออนไลน์ขับเคลื่อนเศรษฐกิจดิจิทัลประเทศ

(มาตรา 43 และร่าง พ.ร.บ.สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ....)

1. ปรับปรุงหลักเกณฑ์ที่มีอยู่เดิม

ม. 5 ปรับปรุง/เพิ่มบทนิยาม

- ปรับปรุงนิยาม “หน่วยงานของรัฐ” เพื่อความชัดเจน ครอบคลุมทั้งองค์การมหาชน หน่วยงานของศาล/รัฐสภา องค์กรตามรัฐธรรมนูญ องค์กรอิสระ
- เพิ่มเติม “ระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติ” ตาม e-Communication Convention Article 4 (g)
- เพิ่มเติม “ผู้อำนวยการ” และ “สำนักงาน” รองรับ ETDA ตามร่าง ETDA

ม. 8 หนังสือ/หลักฐานเป็นหนังสือ

- เพิ่มเติมถ้อยคำ “กำหนดผลทางกฎหมายกรณีไม่ทำเป็นหนังสือ ไม่มีหลักฐานเป็นหนังสือหรือไม่มีเอกสารมาแสดง” ตามแบบ e-Communication Convention (Article 9 วรรค 2)

ม. 9 ลายมือชื่ออิเล็กทรอนิกส์

- เพิ่มเติมถ้อยคำ “กำหนดผลทางกฎหมายกรณีที่ไม่มีการลงลายมือชื่อไว้” ตามแบบ e-Communication Convention (Article 9 วรรค 3)
- เพิ่มเติมเกณฑ์พิจารณาวิธีการทำ e-signature โดยวิธีอื่นใด (นอกจากวิธีการที่เชื่อถือได้) โดยพิจารณาจากวิธีการนั้นเองหรือพยานหลักฐานอื่น ตามแบบ e-Communication Convention (Article 9 วรรค 3 (b))

1. ปรับปรุงหลักเกณฑ์ที่มีอยู่เดิม (ต่อ)

ม. 16 หลักเกณฑ์พิจารณาว่าข้อมูลเป็นของผู้ส่งหรือไม่

- ปรับปรุง (1) โดยกำหนดให้ตรวจสอบตาม “วิธีการที่ผู้ส่งข้อมูลได้ตกลงหรือผูกพันตนไว้ว่าเป็นข้อมูลอิเล็กทรอนิกส์ของผู้ส่งข้อมูล” จากเดิมต้องเป็นวิธีการที่ผู้ส่งและผู้รับตกลงกันเท่านั้น

ม. 26 ลายมือชื่ออิเล็กทรอนิกส์

- ปรับปรุงถ้อยคำใน (4) โดยตัดคำว่า “ในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่อ~~อิเล็กทรอนิกส์~~ เป็นไปเพื่อรับรองความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์” ออก

2. Harmonize Law with UN E-Communication Convention

(United Nations Convention on the Use of Electronic. Communications in International Contracts)

เพิ่มเติมหลักเกณฑ์รองรับ

ม. 13/1 Invitations to make offers

กำหนดให้การเสนอเพื่อทำสัญญาผ่านการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ที่ไม่ได้ส่งถึงบุคคลใดโดยเฉพาะเจาะจง โดยหลักให้ถือเป็นคำเชิญชวนเพื่อทำคำเสนอ

ม. 13/2 Automatic Data System

รองรับผลทางกฎหมายของการทำสัญญาผ่านระบบข้อมูลอัตโนมัติ ที่แม้ไม่มีบุคคลธรรมดาแทรกแซง

ม. 17/1 Input Error

รองรับการแก้ไขเจตนากรณีมีการลงข้อมูลผิดพลาดโดยบุคคลธรรมดาที่ส่งผ่านระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติ ซึ่งไม่มีช่องทางให้บุคคลดังกล่าวแก้ไขข้อผิดพลาดที่เกิดขึ้น

3. ปรับปรุงกลไกการดูแลธุรกิจบริการ และบทกำหนดโทษ

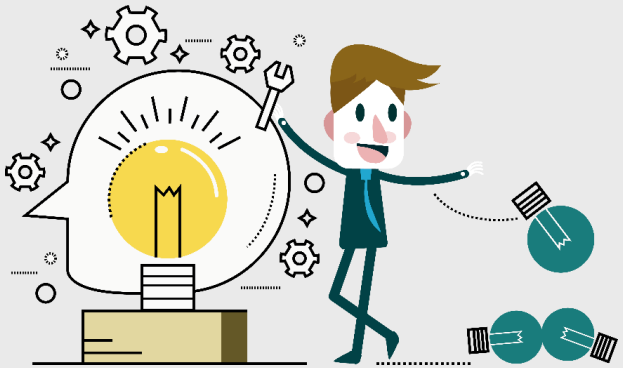
- กำหนดหน่วยงานหลักในการกำกับดูแล โดยให้ ETDA เป็นหลัก เว้นแต่จะมอบหน่วยงานอื่น (ม.32)
- ปรับปรุงขั้นตอนการกำกับดูแลให้ชัดเจนและครบขั้นตอน ทั้งแจ้งให้ทราบ ขั้นทะเบียน ขออนุญาต พร้อม SLA ในการทำงานของเจ้าหน้าที่ (ม.33 , ม. 33/1 , ม. 34)
- รองรับการออกเกณฑ์ที่เป็นกฎหมายลูกรองจาก พ.ร.ฎ. โดยหน่วยงานกำกับดูแลที่ได้รับมอบหมาย (ม.34/1)
- เพิ่มเติมหน้าที่ของพนักงานเจ้าหน้าที่เพื่อคุ้มครองผู้ใช้บริการ (ม. 34/2) เช่น ขอให้ให้ข้อมูล เข้าไปในสถานที่
- ปรับปรุงอัตราโทษให้เหมาะสมกับประเภทการกำกับดูแล (ม.44 , ม. 44/1 , ม. 45)

มีความผิดเฉพาะ

- ประกอบธุรกิจโดยไม่แจ้งให้ทราบ ขึ้นทะเบียน ขออนุญาต
- ประกอบธุรกิจโดยฝ่าฝืนคำสั่งให้หยุด ห้าม ระงับ เพิกถอนการแจ้ง/ขึ้นทะเบียน/อนุญาต หรือพักใช้ใบอนุญาต

อัตราโทษ

- ธุรกิจที่แจ้งให้ทราบ โทษไม่เกิน 1 ปี ปรับไม่เกิน 1 แสนบาท
- ธุรกิจที่ขึ้นทะเบียน โทษไม่เกิน 2 ปี ปรับไม่เกิน 2 แสนบาท
- ธุรกิจที่ขออนุญาต โทษไม่เกิน 3 ปี ปรับไม่เกิน 3 แสนบาท



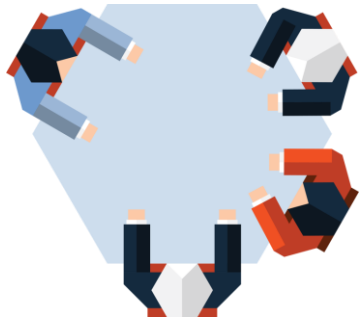
4. ปรับองค์ประกอบและอำนาจหน้าที่ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

(มาตรา 36 – มาตรา 41 และมาตรา 43/1)

- เน้นกรรมการผู้เชี่ยวชาญ เพื่อผลักดันธุรกรรมทางอิเล็กทรอนิกส์

หน้าที่และอำนาจ

- เห็นชอบแผนยุทธศาสตร์เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ พร้อมส่งเสริม สนับสนุน กำกับติดตามให้เป็นไปตามแผน
- กำหนดมาตรฐานด้านเทคโนโลยีดิจิทัลในส่วนที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์
- เสนอแนะต่อ คกก. DE และ ครม. ในการจัดให้มีหรือปรับปรุงกฎหมายที่เกี่ยวข้องกับการพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
- ออกระเบียบหรือประกาศเพื่อให้เป็นไปตามพระราชบัญญัตินี้ หรือเพื่อส่งเสริมและสนับสนุนการทาธุรกรรมทางอิเล็กทรอนิกส์
- กำกับดูแลการประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์



คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

- ผู้ทรงคุณวุฒิ เป็นประธาน (ครม. แต่งตั้ง)
- ปลัด MDES เป็นรองประธาน
- กรรมการผู้ทรงคุณวุฒิ จำนวน 8 คน (ครม. แต่งตั้ง)
- ผู้อำนวยการ สพธอ. กรรมการและเลขา

เชื่อมโยงการทำงานผ่าน ปลัด MDES และผู้อำนวยการ

คณะกรรมการกำกับสำนักงานฯ

- ผู้ทรงคุณวุฒิ เป็นประธาน (รัฐมนตรีแต่งตั้ง)
- ปลัด MDES
- ผู้แทนสำนักงบประมาณ
- กรรมการผู้ทรงคุณวุฒิ จำนวน 6 คน (รัฐมนตรีแต่งตั้ง)
- ผู้อำนวยการ สพธอ. กรรมการและเลขา

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

5. จัดตั้งหน่วยงานเพื่อส่งเสริมธุรกรรมออนไลน์ ขับเคลื่อนเศรษฐกิจดิจิทัล และทำหน้าที่ฝ่ายเลขา คกก.ธุรกรรมฯ

(ม. 43 และร่าง พ.ร.บ. สพธอ. พ.ศ. ....)

สรุปสาระสำคัญ

ร่างกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. ....

- **ที่มา**
  - เดิมมีการจัดทำเป็นกฎหมายใหม่ (ร่าง พ.ร.บ.การพิสูจน์และยืนยันตัวตนทางดิจิทัล พ.ศ. ....) โดยมิได้นำมารวมไว้ในกฎหมายธุรกรรมฯ
  - แต่ คกก.กฤษฎีกา เห็นว่า เรื่องนี้เป็นส่วนหนึ่งของการทำธุรกรรมทางอิเล็กทรอนิกส์ จึงควรรวมไว้ในกฎหมายนี้
- **สำหรับเหตุผลที่รวมไว้ในกฎหมายธุรกรรมทางอิเล็กทรอนิกส์**
  - เนื่องจากการพิสูจน์และยืนยันตัวตนทาง Digital เป็นส่วนหนึ่งของการทำธุรกรรมทางอิเล็กทรอนิกส์
  - อีกทั้งมีความเชื่อมโยงกับการลงลายมือชื่อทางอิเล็กทรอนิกส์ ที่ต้องสามารถระบุตัวตนได้ ดังนั้น e-Signature กับ DID จึงมีความสัมพันธ์เชื่อมโยงกัน

- **หลักการสำคัญ เพิ่มหมวด 3/1 ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล ดังนี้**
  - เพิ่มนิยามคำว่า “การพิสูจน์และยืนยันตัวตน” และ “ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล”
  - ปรับบท รมว. รักษาการ จากเดิม นายก และ รมว. MDES เป็น รมว. MDES คนเดียว เนื่องจากเป็นงานที่ รมว. MDES รับผิดชอบเป็นหลัก และหน่วยงานที่ดูแลเรื่องนี้อยู่ในความรับผิดชอบของ รมว. MDES
  - รองรับการพิสูจน์และยืนยันตัวตนทางดิจิทัล โดยหากทำผ่านระบบฯ จะได้รับข้อสันนิษฐานว่าเป็นบุคคลคนนั้นจริง
  - กำหนดให้มีการกำกับดูแลการให้บริการระบบฯ ในรูปแบบการอนุญาต โดยอาจมี คณะกรรมการชุดเล็กทำหน้าที่

มองจากคนทำงาน DIGITAL ID

1

สร้างมาตรฐานการพิสูจน์และการยืนยันตัวตนของประเทศไทย และยกระดับการทำธุรกรรมต่างๆ ให้มีความน่าเชื่อถือมากขึ้น

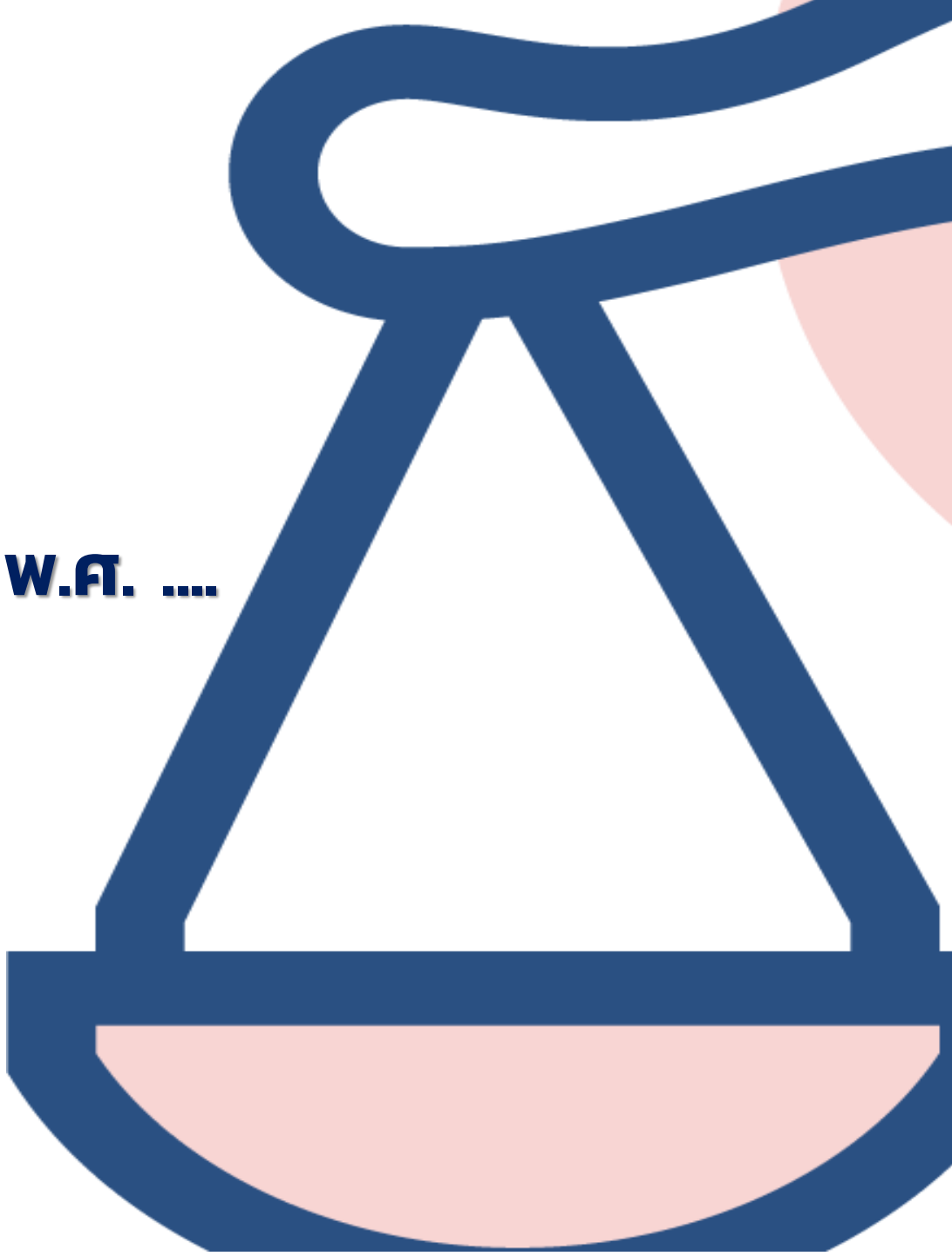
2

สามารถพิสูจน์และยืนยันตัวตนผ่านช่องทาง Online Self Service ได้

3

สร้างระบบ Data Sharing โดยเป็นเพียงถนนเพื่อเชื่อมต่อระหว่างหน่วยงานต่างๆ (ไม่มีการรวมศูนย์เก็บข้อมูล) และการ Share ต้องได้รับการ Consent จากเจ้าของข้อมูลก่อน

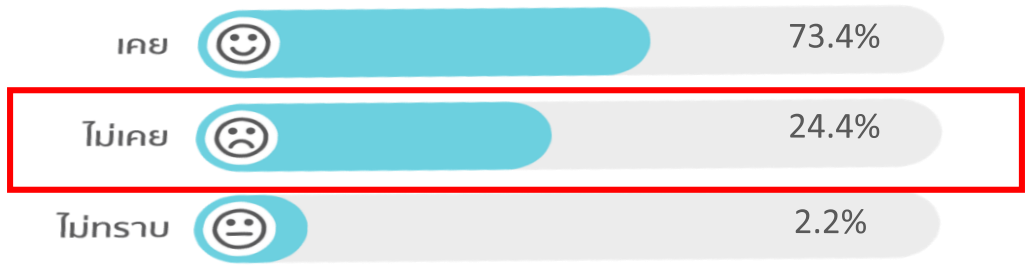
ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....



ผลการสำรวจสถิติ ด้านความตระหนักในการดูแลข้อมูลส่วนบุคคล

เมื่อใช้ Social Media

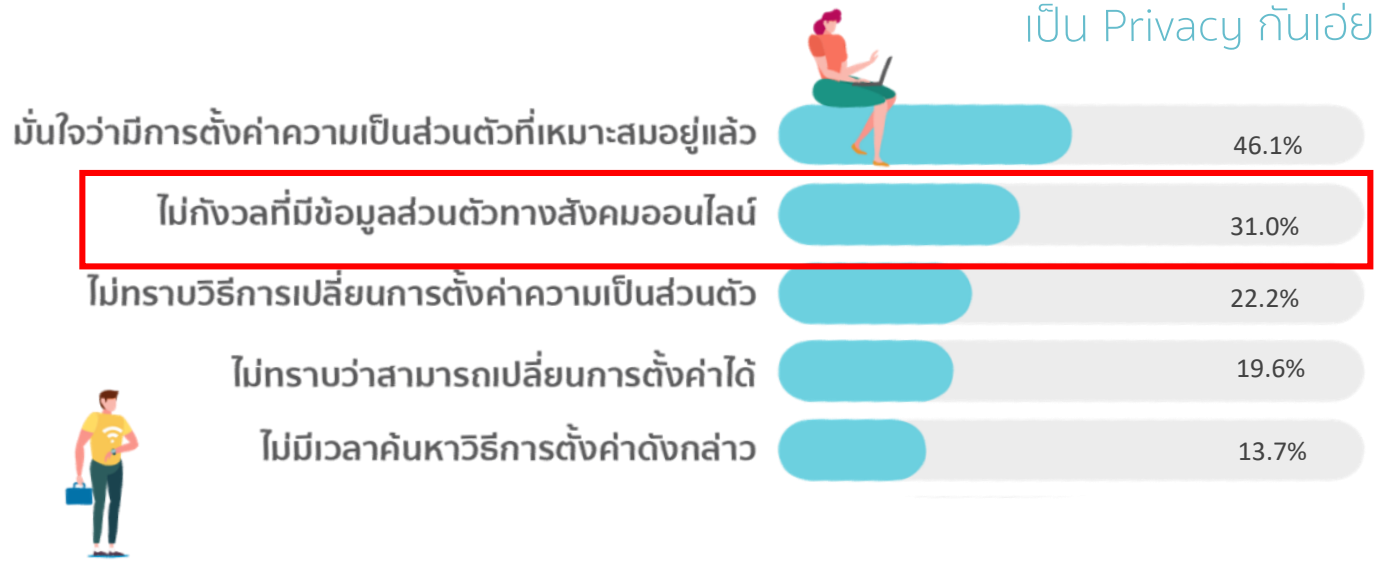
คนไทยตั้งค่าข้อมูลส่วนตัวเป็น Privacy กันไหม



THAILAND INTERNET USER PROFILE 2018

ทำไม ไม่ตั้งค่าข้อมูลส่วนตัว

เป็น Privacy กันเอ่ย

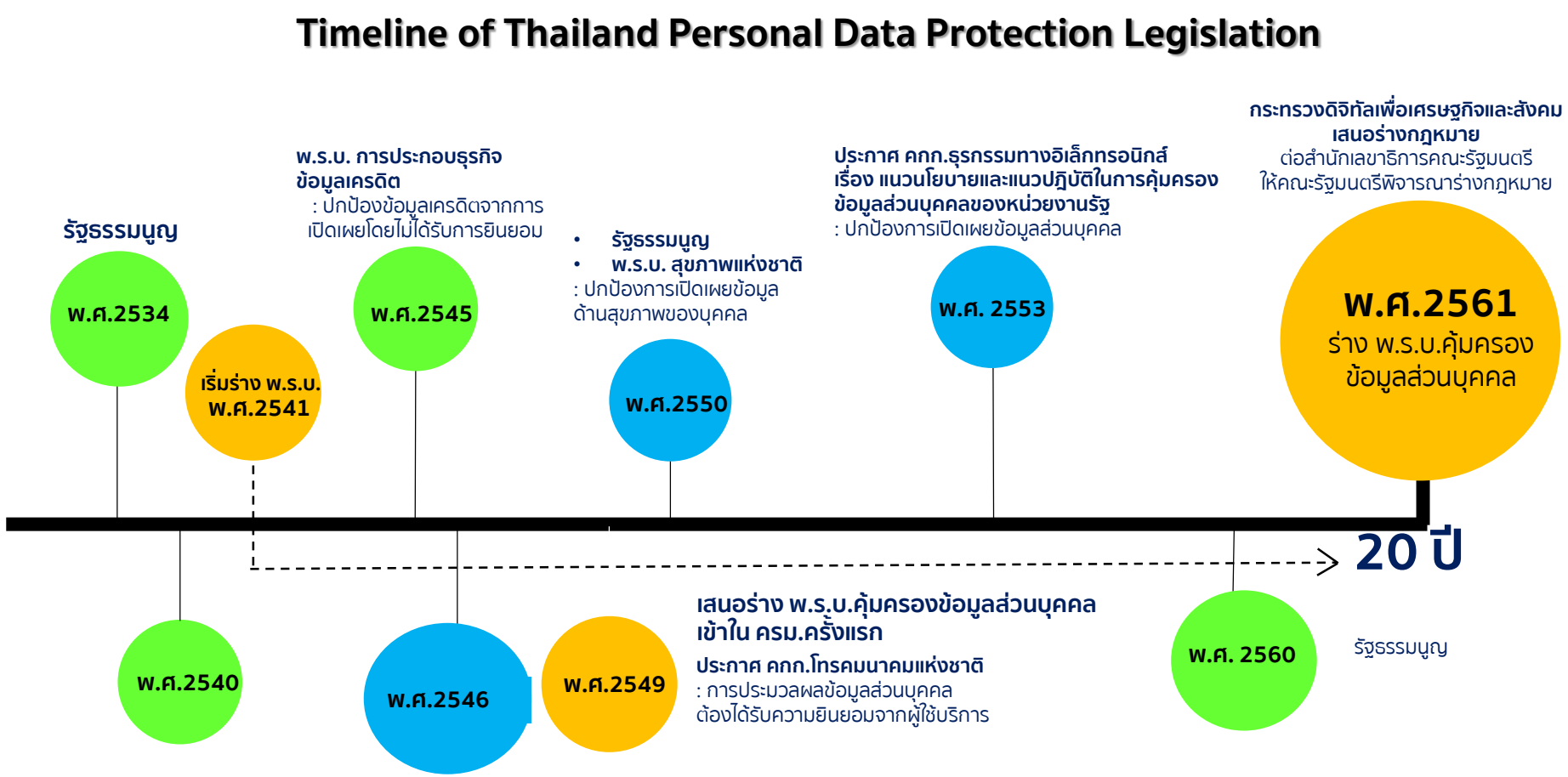


รู้ไหมว่า ทำแบบนี้แล้ว...

ช่างสุ่มเสี่ยงต่อการถูกละเมิดข้อมูลส่วนบุคคลเหลือเกิน

THAILAND INTERNET USER PROFILE 2018

ร่าง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

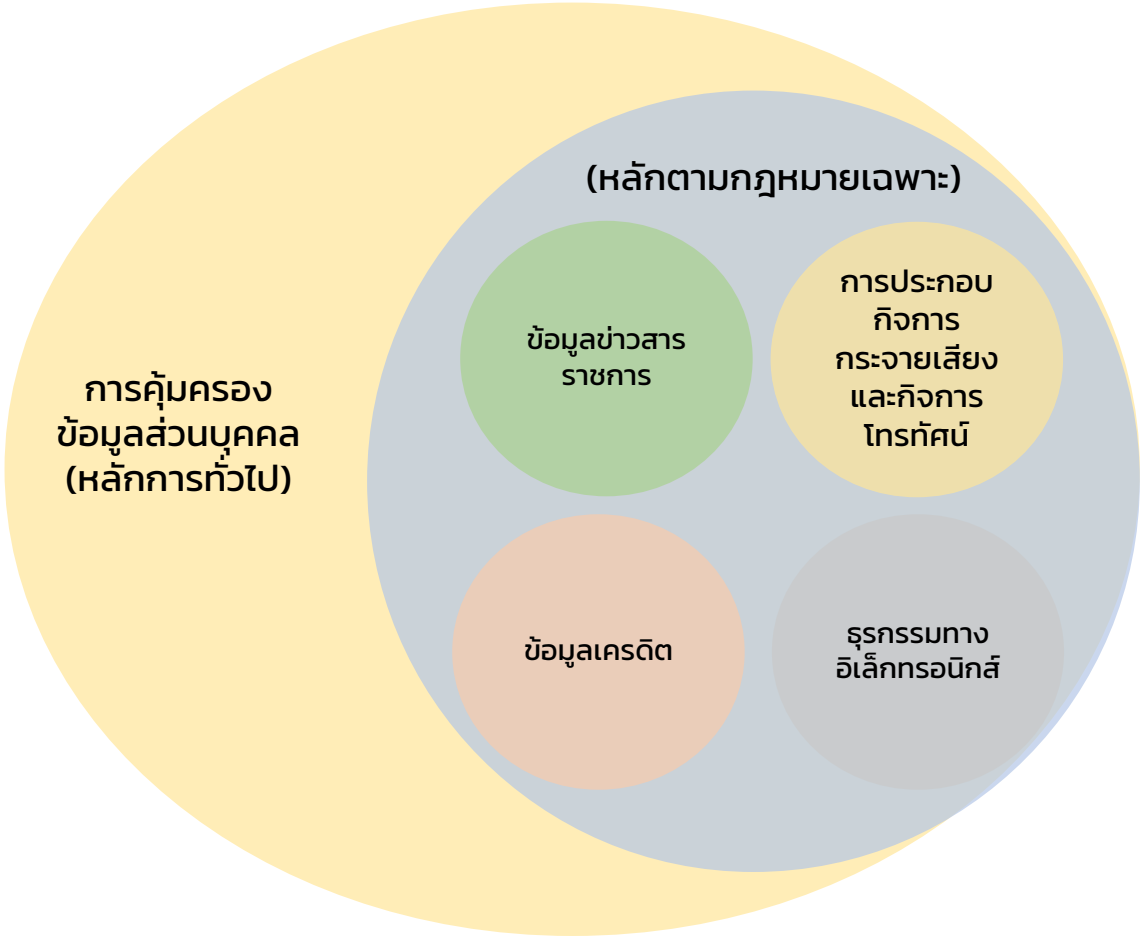


ความสัมพันธ์กับหลักกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามกฎหมายอื่น

“วางหลักทั่วไปและมาตรฐานขั้นต่ำในการคุ้มครองข้อมูลส่วนบุคคล”

ข้อจำกัดของกฎหมายปัจจุบันที่มีอยู่

- มีลักษณะเป็นการบังคับตามเจตนารมณ์และวัตถุประสงค์เฉพาะเรื่อง
- ขาดความเชื่อมโยงกับการใช้งานทางเทคโนโลยี
- กฎหมายบางฉบับมีกลไกในการให้ความคุ้มครองข้อมูลส่วนบุคคลไม่ครบถ้วนทั้งกระบวนการ จึงยังเกิดช่องว่างในการคุ้มครองข้อมูลส่วนบุคคล



กรอบความคิดในการคุ้มครองข้อมูลส่วนบุคคล

1. หลักข้อจำกัดในการเก็บรวบรวมข้อมูล
2. หลักคุณภาพของข้อมูล
3. หลักการกำหนดวัตถุประสงค์ในการจัดเก็บ
4. หลักข้อจำกัดในการนำไปใช้
5. หลักการรักษาความมั่นคงปลอดภัยข้อมูล
6. หลักการเปิดเผยข้อมูล
7. หลักการมีส่วนร่วมของบุคคล
8. หลักความรับผิดชอบ

ร่าง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

สถานะ ผ่านการพิจารณาของคณะกรรมาธิการวิสามัญวาระ 2 เตรียมเสนอเข้า สนช. วาระ 3

ในชั้นการพิจารณาได้นำหลักการของ GDPR ซึ่งเป็นกฎหมายด้านการคุ้มครองข้อมูลส่วนบุคคลของ EU มาเป็นแนวทางในการปรับปรุงร่างกฎหมาย เนื่องจากส่งผลกระทบในวงกว้าง

1. บททั่วไป	• บังคับใช้**เมื่อพ้น 1 ปี** นับแต่วันประกาศในราชกิจจานุเบกษา • **เว้นแต่** เรื่อง**คณะกรรมการ สำนักงาน**และ**บทเฉพาะกาล** ที่ให้ใช้**บังคับนับแต่วันประกาศในราชกิจจานุเบกษา** • รัฐมนตรี DE เป็นผู้รักษาการตามกฎหมาย
2. คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	• คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล จำนวน 17 คน (ประธาน และกรรมการผู้ทรงคุณวุฒิ มาจากการสรรหา)
	อำนาจหน้าที่ • จัดทำแผนแม่บทด้านการส่งเสริม หลักเกณฑ์ที่จำเป็น รวมถึงแนวปฏิบัติที่สำคัญในการคุ้มครองข้อมูลส่วนบุคคล • ให้คำแนะนำ ปรึกษา และวินิจฉัยปัญหาที่เกิดจากการบังคับใช้กฎหมาย
3. สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	**คณะกรรมการกำกับสำนักงาน** • องค์ประกอบ : ประธาน กรรมการโดยตำแหน่ง และกรรมการผู้ทรงคุณวุฒิ จำนวน 10 คน (ประธานและผู้ทรงคุณวุฒิมาจากการสรรหา) • อำนาจหน้าที่ : กำกับการดำเนินงานของสำนักงานฯ ให้เป็นไปตามแผนหรือเป้าหมาย
	เลขาธิการสำนักงาน • มาจากการสรรหา และแต่งตั้ง โดยคณะกรรมการกำกับสำนักงาน • ทำหน้าที่ในการบริหารจัดการงานของสำนักงาน
	อำนาจหน้าที่ของสำนักงาน • ร่างแผนแม่บทมาตรการแก้ไขปัญหาและอุปสรรคในการปฏิบัติงาน • ศึกษา วิจัย พัฒนาเทคโนโลยีที่เกี่ยวข้อง รวมถึงการวิเคราะห์ด้านมาตรฐานที่เกี่ยวข้อง • เป็นศูนย์กลางข้อมูลและการให้บริการทางวิชาการ การฝึกอบรม และการให้คำปรึกษา • สำรวจ จัดทำสถิติ ติดตามความเคลื่อนไหวของสถานการณ์และแนวโน้มการเปลี่ยนแปลง

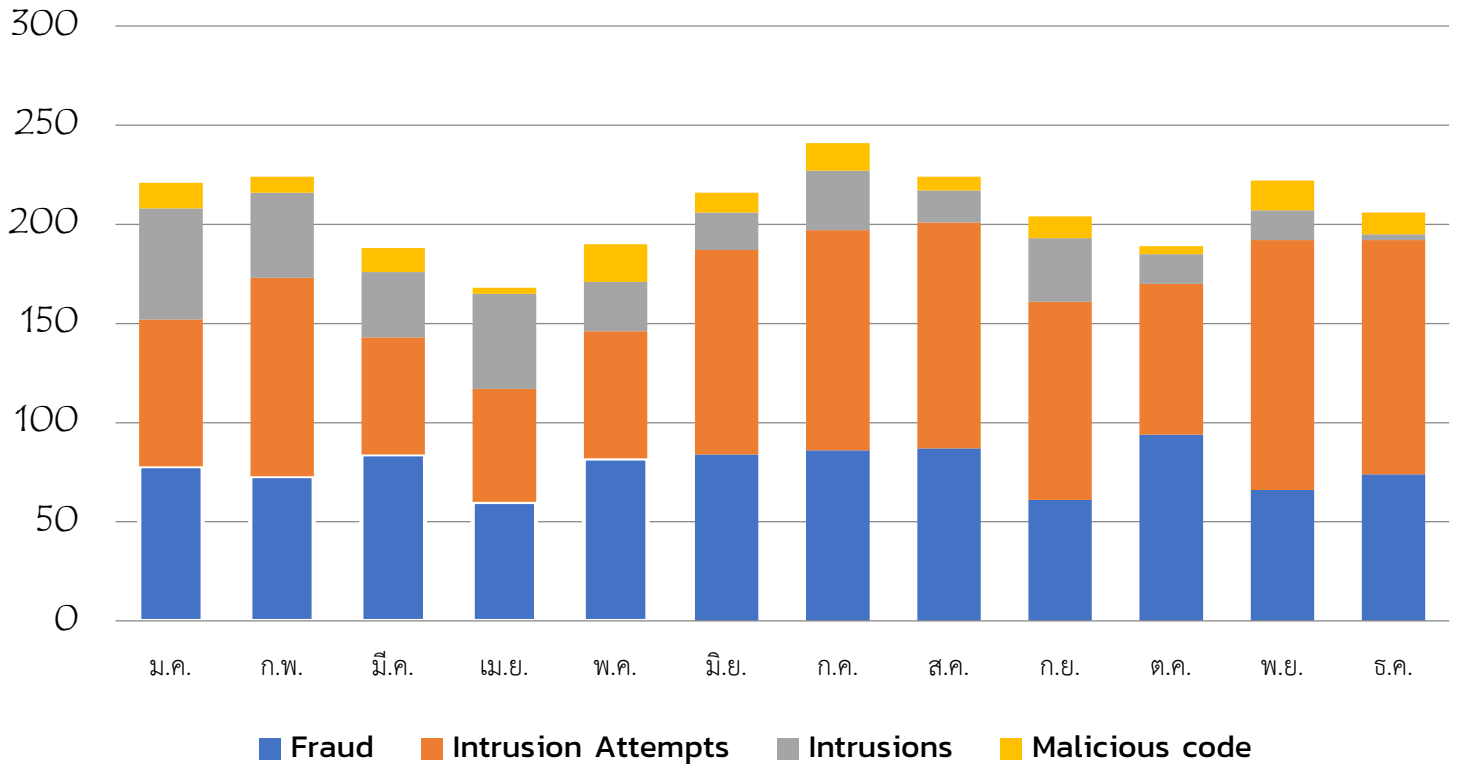
4. หลักการคุ้มครองข้อมูลส่วนบุคคล	• กรณีมีกฎหมายอื่นกำหนดเรื่องการคุ้มครองข้อมูลส่วนบุคคลไว้ ให้เป็นไปตามกฎหมายนั้น • เว้นแต่การ**เก็บรวบรวม ใช้ เปิดเผย สิทธิของเจ้าของข้อมูล และการร้องเรียน ให้เป็นไปตามกฎหมายนี้**
	• กำหนดข้อยกเว้นการบังคับใช้กฎหมายนี้ เช่น เพื่อประโยชน์ส่วนตัว หรือเพื่อกิจกรรมในครอบครัวของบุคคลเท่านั้น
	• **กำหนดหลักเกณฑ์**ในขั้นตอนการเก็บรวบรวม การใช้ การเปิดเผย การโอนข้อมูลระหว่างประเทศ สิทธิของเจ้าของข้อมูล ข้อยกเว้น รวมทั้งข้อจำกัดการคุ้มครองข้อมูลและสิทธิของเจ้าของข้อมูล
5. กลไกการดำเนินงาน	**คณะกรรมการผู้เชี่ยวชาญ** • **พิจารณาเรื่องร้องเรียน**กรณีมีการฝ่าฝืนการดำเนินการตามกฎหมายนี้ • ติดตามบังคับการดำเนินการตามมติ คกก. ผู้เชี่ยวชาญ
	• มีขั้นตอนการ**ไกล่เกลี่ยข้อพิพาท**เกี่ยวกับข้อมูลส่วนบุคคล สำหรับเรื่องที่ไกล่เกลี่ยได้
	• มีการกำหนดโทษทางอาญา และโทษปรับทางปกครอง • เพิ่มเติมเรื่อง **ค่าเสียหายในเชิงลงโทษ**
7. บทเฉพาะกาล	**การทำงานระยะแรก** • ตั้งคณะกรรมการระดับชาติชุดแรกตั้ง ให้ปฏิบัติหน้าที่ไปพลางก่อน • ให้ ครม. จัดสรรทุนประเดิมแก่สำนักงานตามความจำเป็น
	ข้อมูลส่วนบุคคลที่**เก็บรวบรวมไว้ก่อนกฎหมายนี้ใช้บังคับ ให้ใช้ต่อไปได้ แต่ต้องเพิ่มเติมเรื่องการยกเลิกความยินยอม**

4

ภัยคุกคามทางไซเบอร์

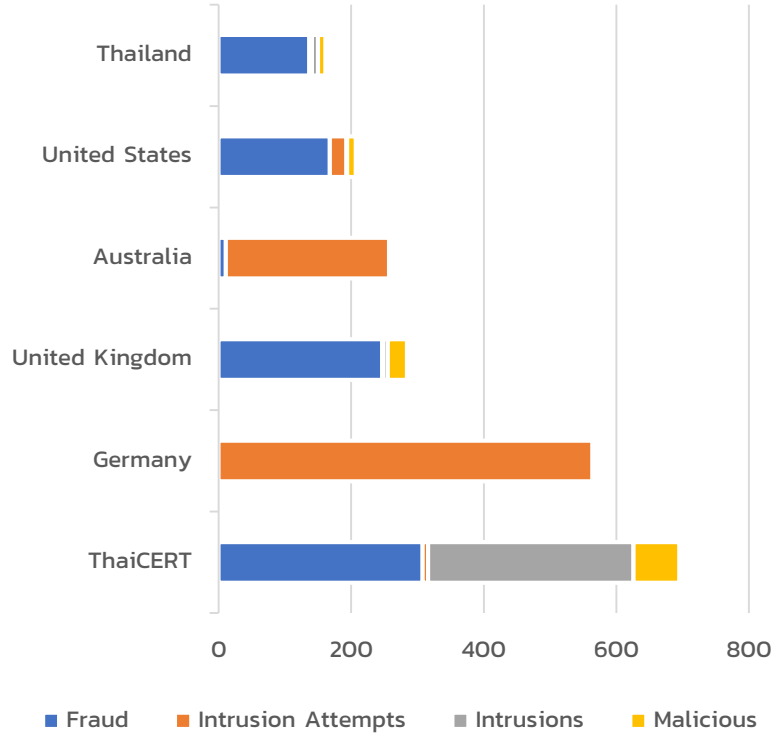
สถิติการรับแจ้งเหตุภัยคุกคามของไทยเซิร์ต ปี 2561

จำนวนภัยคุกคามไซเบอร์ที่ไทยเซิร์ตได้รับแจ้งและดำเนินการทั้งสิ้น **2,520** กรณี
โดย **ภัยคุกคามที่ได้รับแจ้งมากที่สุด** คือ **Intrusion Attempts** และ **Fraud** โดยมีอัตราส่วนถึง 43% และ 36% ตามลำดับ



ข้อมูลตั้งแต่เดือน ม.ค. – ธ.ค. 2561

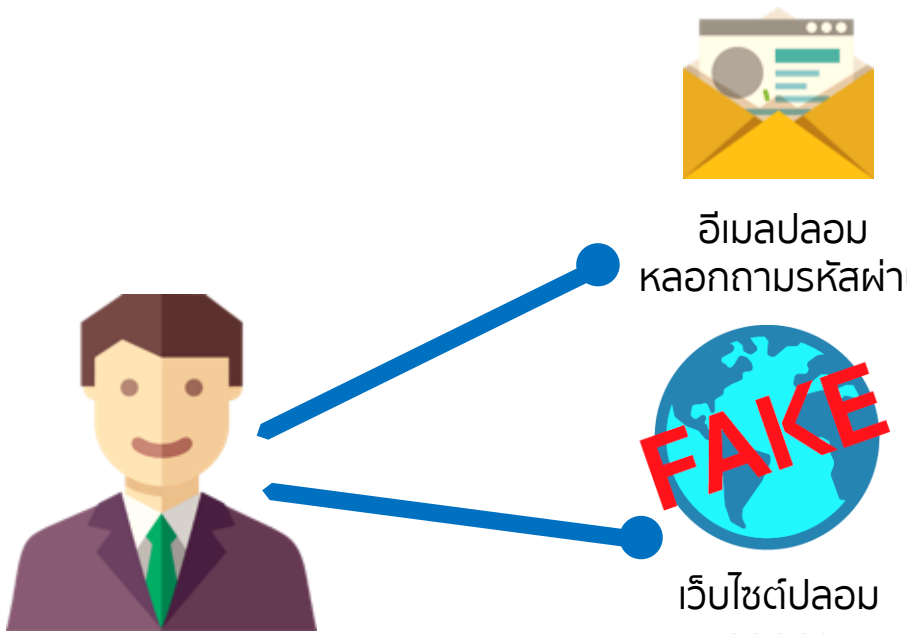
6 อันดับประเทศที่แจ้งเหตุภัยคุกคามมากที่สุด



ระบบ Threat Watch ไทยเซิร์ตพัฒนาขึ้นมาเอง เป็นการรวบรวมข้อมูลจากแหล่งข้อมูลสาธารณะที่มีการประกาศแจ้งรายชื่อระบบ ที่ถูกโจมตี ข้อมูลที่แลกเปลี่ยนกันระหว่างเครือข่ายหน่วยงาน CERT และรายงานจากระบบตรวจวิเคราะห์ภัยคุกคามอื่น ๆ

- Intrusion Attempts คือ ภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ
- Fraud คือ ภัยคุกคามที่พยายามการหลอกลวงเพื่อผลประโยชน์ เช่น การสร้างเว็บหลอกลวง (Phishing Site)
- Intrusions คือ ภัยคุกคามที่เกิดกับระบบที่ถูกเจาะได้สำเร็จ เช่น การเปลี่ยนหน้าเว็บไซต์ (Web Defacement)
- Malicious Code คือ ภัยคุกคามที่เกิดจากเผยแพร่โปรแกรมไม่พึงประสงค์ เช่น การแทรก source code อันตรายบนหน้าเว็บไซต์ (Malicious Site)

ตัวอย่างภัยคุกคามที่เกิดขึ้นบ่อย



อีเมลปลอม
หลอกถามรหัสผ่าน

เว็บไซต์ปลอม
หลอกถาม
รหัสผ่าน

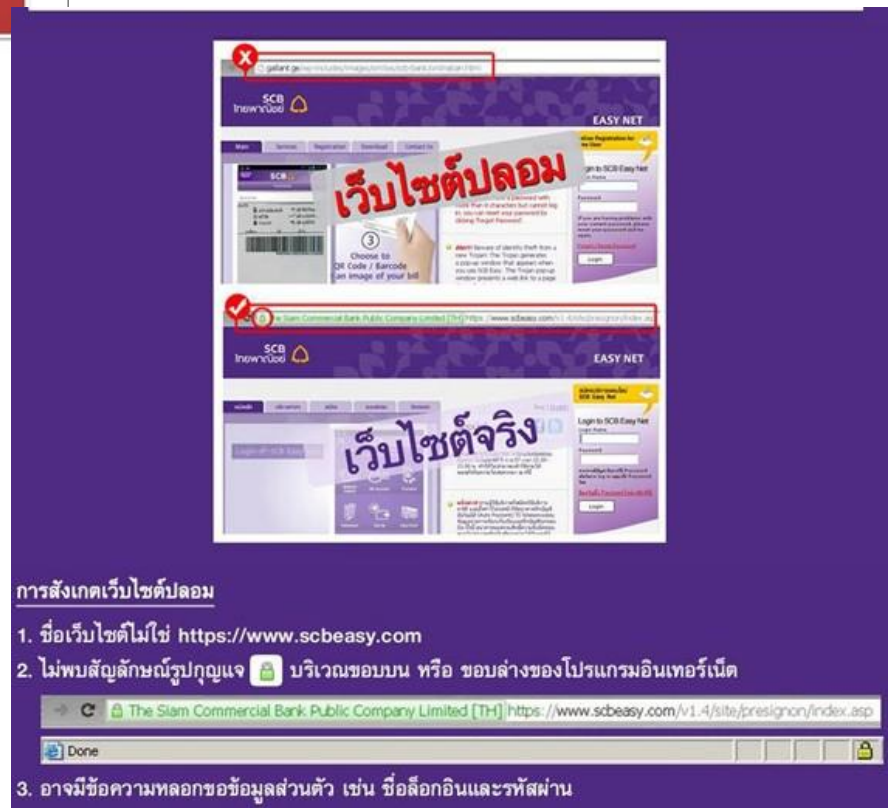
วิธีป้องกัน

- ตรวจสอบ URL ของเว็บไซต์ก่อนล็อกอิน
- ตรวจสอบที่อยู่อีเมลของผู้ส่ง
- ไม่ใช้รหัสผ่านเดียวกันในหลายบริการ
- อีเมล Phishing มักจะใช้ภาษาไม่น่าเชื่อถือ

เช่น สะกดผิด ใช้ภาษาไม่เป็นทางการ

“ปลอมแปลง-หลอก-ฉ้อโกง” ทางออนไลน์

รูปที่ 1 ประกาศใน Twitter ของธนาคารไทยพาณิชย์



กรณี ปลอมอีเมลหลอกให้โอนเงิน

1 ผู้ซื้อกับผู้ขายติดต่อซื้อขายสินค้าผ่านอีเมล โจรสามารถดักอ่านการสนทนาของทั้งสองฝ่ายได้

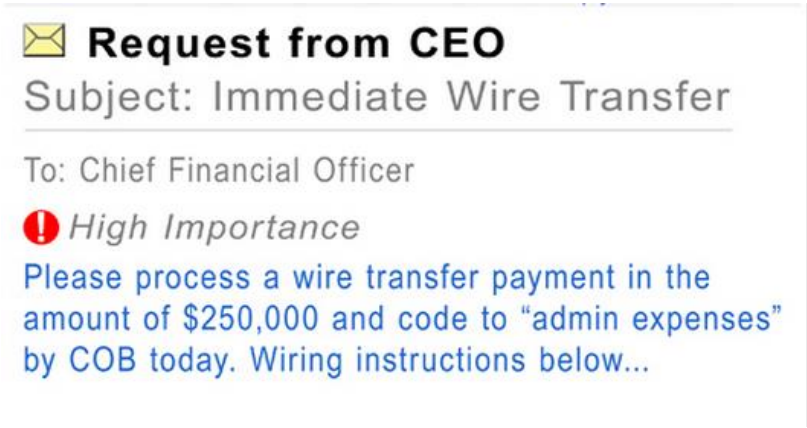
2 ในขณะที่กำลังจะตกลงซื้อขาย โจรปลอมอีเมลหลอกให้ผู้ซื้อโอนเงินมาที่บัญชีธนาคารของโจร

3 ผู้ซื้อหลงเชื่อและโอนเงินเข้าบัญชีธนาคารของโจร

กรณี ปลอมอีเมลหลอกให้โอนเงิน

Case study
Business Email Compromise (BEC)

- เจ้าหน้าที่บัญชีได้รับอีเมลจาก CEO ระหว่างที่ CEO เดินทางต่างประเทศ แจ้งให้โอนเงินด่วนภายในเวลาทำการ (COB) และอ้างว่าฝ่ายกฎหมายจะแจ้งรายละเอียดเพิ่มเติม
- ต่อมา เจ้าหน้าที่บัญชีคนดังกล่าวได้รับอีเมลอีกฉบับจากฝ่ายกฎหมายที่ให้รายละเอียดเกี่ยวกับการโอนเงินเพิ่มเติม และได้รับหนังสือมอบอำนาจที่ลงนามด้วย CEO และตราประทับบริษัท
- เจ้าหน้าที่บัญชีจึงโอนเงิน 737,000 $ USD ไปยังธนาคารที่จีน
- วันต่อมา CEO โทรศัพท์คุยกับเจ้าหน้าที่บัญชีคนดังกล่าว เจ้าหน้าที่บัญชีจึงได้พูดถึงเรื่องการโอนเงิน จึงได้ทราบว่า CEO ไม่เคยส่งอีเมลมาก่อน



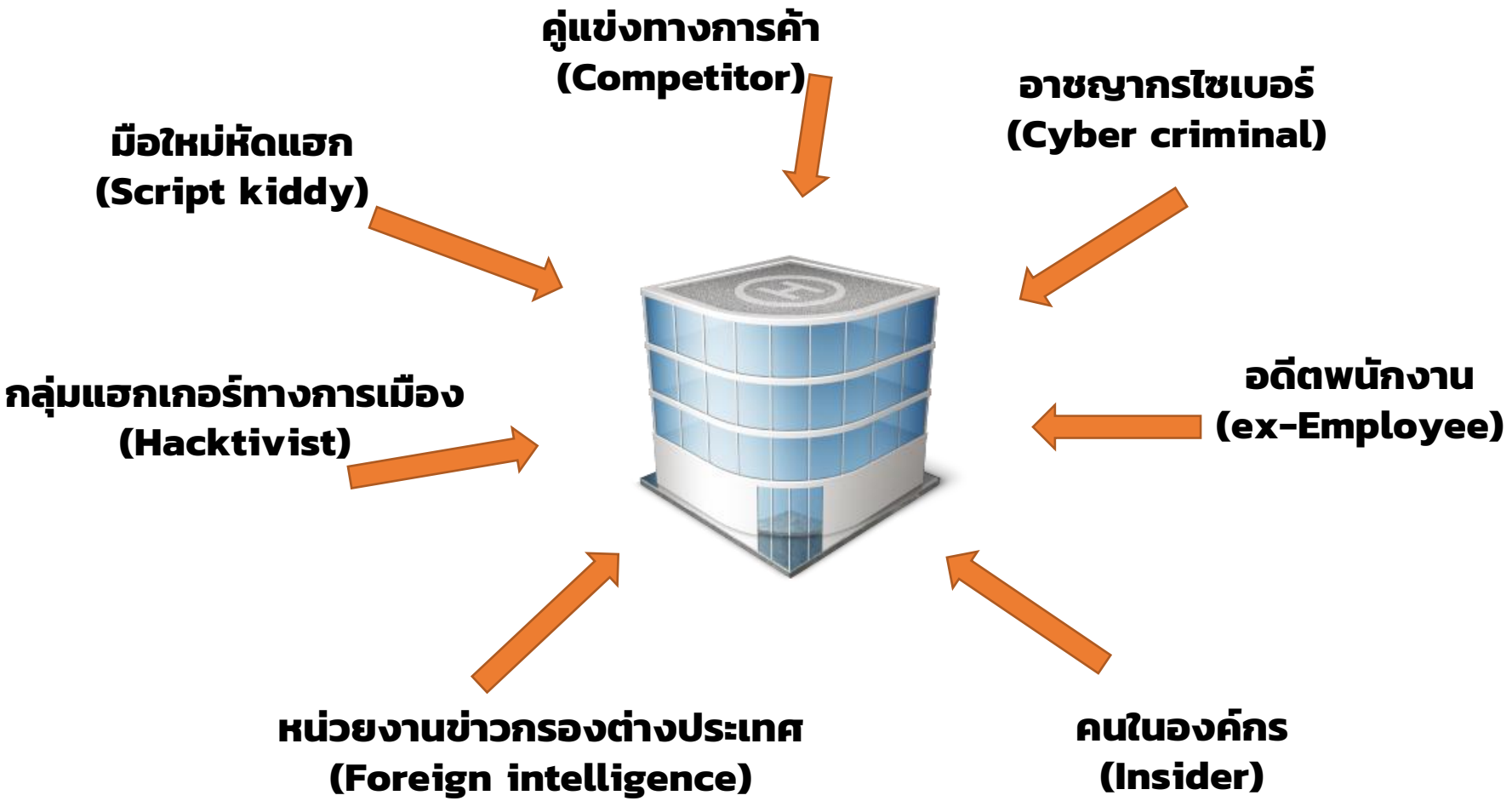
FBI's Internet Crime Complaint Center (FBI IC3)
2013 – กว่า 7,000 บริษัทในสหรัฐอเมริกาตกเป็นเหยื่อ มูลค่าความเสียหาย เกินกว่า 740 ล้าน USD (ไม่รวมเหยื่อนอกสหรัฐอเมริกา)

2015 – ยอดผู้ตกเป็นเหยื่อ BEC เพิ่มขึ้นอีก 270 % มาจากทั้ง 50 รัฐ และกว่า 80 ประเทศทั่วโลกตกเป็นเหยื่อ

ที่มา https://www.fbi.gov/

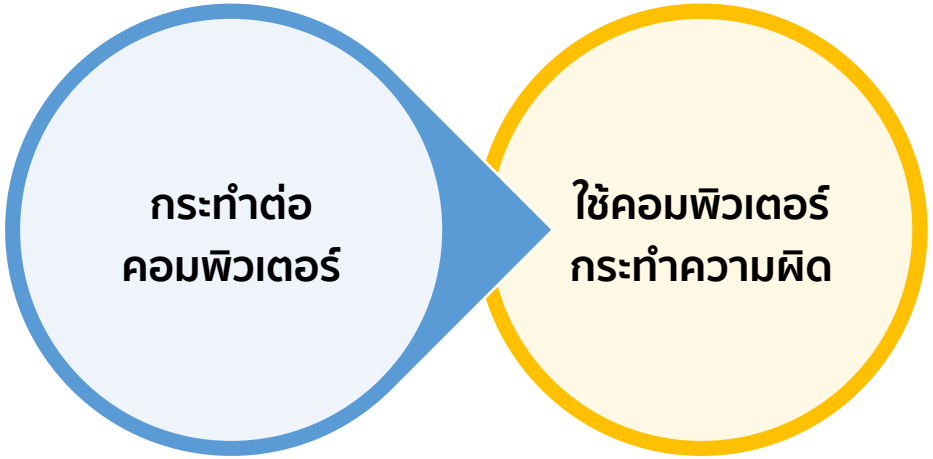
- ✓ **พบว่า email มาจาก .co แทน .com,**
- ✓ **ลายมือชื่อและตราประทับปลอม,**
- ✓ **คนร้ายทราบตารางงาน CEO จากข่าว event ของบริษัท**

ตัวอย่างประเภทของผู้โจมตี



พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550



กำหนดมาตรการในการ ***ป้องกันและปราบปราม*** การกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ความผิดตาม พ.ร.บ.คอมพิวเตอร์ฯ

กระทำต่อคอมพิวเตอร์

- เข้าถึงระบบคอมฯ (ม.5)
- ล่วงรู้มาตรการป้องกันการเข้าถึง (ม.6)
- เข้าถึงข้อมูลคอมฯ (ม.7)
- ดักรับข้อมูลคอมฯ (ม.8)
- รบกวนข้อมูลคอมฯ (ม.9)
- รบกวนระบบคอมฯ (ม.10)
- จำหน่าย/เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด (ม.13)

ใช้คอมพิวเตอร์กระทำความผิด

- Spam mail (ม.11)
- ปลอมข้อมูลคอมพิวเตอร์/เผยแพร่เนื้อหาไม่เหมาะสม (ม.14)
- ความรับผิดของผู้ให้บริการ (ม.15)
- การเผยแพร่ภาพจากการตัดต่อ/ดัดแปลง (ม.16)
- มาตรการดำเนินการตามคำสั่งศาล (ม.16/1)

ม. 12 บทหนักของมาตรา 5, 6, 7, 8, 11

ม. 12/1 บทหนักของมาตรา 9, 10

Hacking

ข้อมูลคอมพิวเตอร์

ม. 5

- ❑ เข้าถึง
- ❑ โดยมิชอบ
- ❑ ระบบคอมฯ ที่มาตรการป้องกันที่มิใช่มีไว้สำหรับตน

* จำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 10,000 บาท หรือทั้งจำทั้งปรับ

ระบบคอมพิวเตอร์

ม. 7

- ❑ เข้าถึง
- ❑ โดยมิชอบ
- ❑ ข้อมูลคอมพิวเตอร์ ที่มาตรการป้องกันการเข้าถึงที่มิใช่มีไว้สำหรับตน

* จำคุกไม่เกิน 2 ปี ปรับไม่เกิน 40,000 บาท หรือทั้งจำทั้งปรับ

รู้ Password แล้วเปิดเผย

เช่น keylogger

ม. 6

- ❑ รู้มาตรการป้องกันการเข้าถึงระบบคอมของผู้อื่น
- ❑ นำไปเปิดเผยโดยมิชอบ
- ❑ ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

* จำคุกไม่เกิน 1 ปี ปรับไม่เกิน 20,000 บาท หรือทั้งจำทั้งปรับ

แอบดักข้อมูลระหว่างส่ง

เช่น ดักอีเมล์

ม. 8

- ❑ กระทำการโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์
- ❑ เพื่อดักรับข้อมูลของผู้อื่น
- ❑ ที่อยู่ในระหว่างการส่งในระบบคอมฯ
- ❑ ข้อมูลนั้นไม่ได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์

* จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 60,000 บาท หรือทั้งจำทั้งปรับ

แก้ไขข้อมูลคอมพิวเตอร์ผู้อื่น

เช่น malware

ม. 9

- ❑ ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติม
- ❑ ข้อมูลคอมพิวเตอร์ของผู้อื่น
- ❑ ไม่ว่าทั้งหมดหรือบางส่วน
- ❑ โดยมิชอบ

* จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

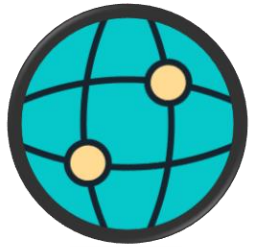
รบกวนระบบคอมพิวเตอร์

เช่น Ddos

ม. 10

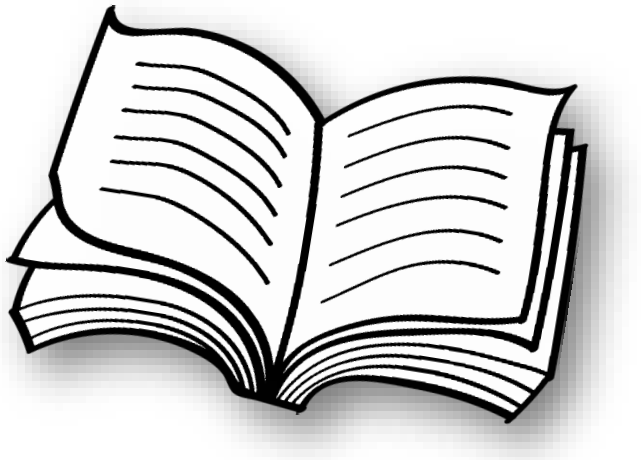
- ❑ ขัดขวางการทำงานของระบบคอมพิวเตอร์ของผู้อื่น
- ❑ โดยมิชอบ
- ❑ เพื่อให้ระบบคอมพิวเตอร์ระงับ ชะลอ ขัดขวาง รบกวน
- ❑ จนไม่สามารถทำงานตามปกติได้

* จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ



ภาพรวม พ.ร.บ. คอมฯ ฉบับที่ 2 ปี 2560

- ผลใช้บังคับ วันที่ ๒๔ พฤษภาคม ๒๕๖๐



SPAM

ปกปิดแหล่งที่มา

ม. 11

ว. 1

- ❑ ส่งข้อมูลหรือจดหมายอิเล็กทรอนิกส์
- ❑ แก่ผู้อื่น
- ❑ โดยปกปิดแหล่งที่มา
- ❑ เป็นเหตุให้รบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น

*ปรับไม่เกิน 100,000 บาท

เพิ่มเติมกรณี ดูแล Privacy :

- **เอาผิด** กับผู้ส่ง SPAM ที่ไม่เปิดโอกาสให้ผู้รับ **ปฏิเสธ** ได้โดยง่าย

และ **ก่อให้เกิดความรำคาญ**

ม.11 SPAM

ว. 2

- ❑ ส่งข้อมูลหรือจดหมายอิเล็กทรอนิกส์
- ❑ แก่ผู้อื่น
- ❑ มีลักษณะก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ
- ❑ ไม่เปิดโอกาสให้บอกเลิก เพื่อปฏิเสธการตอบรับได้โดยง่าย

*ปรับไม่เกิน 200,000 บาท

ออกประกาศเพิ่มหลักเกณฑ์ :

- แค่ไหน เพียงใด **ไม่เป็น SPAM**

ม. 14 (1) นำเข้า / เผยแพร่ข้อมูล

ปรับเจตนารมณ์:

ตัดหมิ่นประมาทออกชัดเจน แล้วเอาผิดกับ

- ✓ ฉ้อโกง (Phishing)
- ✓ ข้อมูลปลอม / บิดเบือน ทั้งหมดหรือบางส่วน
- ✓ ข้อมูลเป็นเท็จ ที่ไม่ใช่หมิ่นประมาทตาม ประมวลกฎหมายอาญา

ไม่ละเมิดสิทธิคนอื่น

หมิ่นประมาท
Hate speech
Cyber Bullying

ความผิดฐานหมิ่นประมาท

มาตรา ๓๒๖ ผู้ใดใส่ความผู้อื่นต่อบุคคลที่สาม โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นหรือถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาท **ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ**

มาตรา ๓๒๗ ผู้ใดใส่ความผู้ตายต่อบุคคลที่สาม และการใส่ความนั้นน่าจะเป็นเหตุให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่นหรือถูกเกลียดชัง ผู้นั้นกระทำความผิดฐานหมิ่นประมาท ต้องระวางโทษดังบัญญัติไว้ในมาตรา ๓๒๖ นั้น

มาตรา ๓๒๘ ถ้าความผิดฐานหมิ่นประมาทได้กระทำโดยการโฆษณาด้วยเอกสาร ภาพวาด ภาพระบายสี ภาพยนตร์ ภาพหรือตัวอักษรที่ทำให้ปรากฏไม่ว่าด้วยวิธีใด ๆ แผ่นเสียง หรือสิ่งบันทึกเสียง บันทึกภาพ หรือบันทึกอักษร กระทำโดยการกระจายเสียง หรือการกระจายภาพ หรือโดยกระทำการป่าวประกาศด้วยวิธีอื่น ผู้กระทำต้อง **ระวางโทษจำคุกไม่เกินสองปี และปรับไม่เกินสองแสนบาท**

ข้อยกเว้นไม่ผิดหมิ่นประมาท

มาตรา ๓๒๙ ผู้ใดแสดงความคิดเห็นหรือข้อความใด**โดยสุจริต**

(๑) เพื่อความชอบธรรม ป้องกันตนหรือป้องกันส่วนได้เสียเกี่ยวกับตนตามคลองธรรม

(๒) ในฐานะเป็นเจ้าพนักงานปฏิบัติการตามหน้าที่

(๓) ติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ หรือ

(๔) ในการแจ้งข่าวด้วยความเป็นธรรมเรื่องการดำเนินการอันเปิดเผยในศาลหรือในการประชุม

ผู้นั้นไม่มีความผิดฐานหมิ่นประมาท

มาตรา ๓๓๐ ในกรณีหมิ่นประมาท ถ้าผู้ถูกหาว่ากระทำความผิด พิสูจน์ได้ว่าข้อที่หาว่าเป็นหมิ่นประมาทนั้นเป็นความจริง ผู้นั้นไม่ต้องรับโทษ

แต่ห้ามไม่ให้พิสูจน์ ถ้าข้อที่หาว่าเป็นหมิ่นประมาทนั้นเป็น**การใส่ความในเรื่องส่วนตัว และการพิสูจน์จะไม่เป็นประโยชน์แก่ประชาชน**

นำเข้า เผยแพร่ ส่งต่อ ข้อมูลคอมพิวเตอร์

ม. 14

- ❑ บิดเบือน ปลอม เท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน ด้วยเจตนาทุจริต หลอกลวง อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

  * แต่ถ้าทำต่อบุคคลใดบุคคลหนึ่ง รับโทษไม่เกิน 3 ปี ปรับไม่เกิน 60,000 บาท ทั้งจำทั้งปรับ

- ❑ เท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ /สาธารณะ / เศรษฐกิจของประเทศ / โครงสร้างพื้นฐานของประเทศ / ก่อให้เกิดความตื่นตระหนกแก่ประชาชน

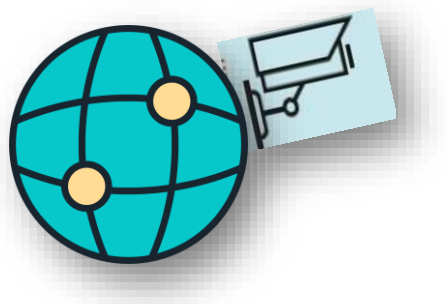
- ❑ เป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้าย ตามประมวลกฎหมายอาญา

- ❑ มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

- ❑ เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑)(๒) (๓) หรือ (๔)

  * จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

ความรับผิดของผู้ให้บริการ



ม. 15

- ผู้ให้บริการ รับผิด ต่อเมื่อ
  - X ให้ความร่วมมือ
  - X ยินยอม
  - X รู้เห็นเป็นใจ

  กับการกระทำความผิดตามมาตรา 14
- เพิ่มกลไก ยกเว้นความรับผิดผู้ให้บริการ ในฐานะตัวกลาง เมื่อ
  - ✓ ทำตามขั้นตอนการแจ้งเตือน
  - ✓ การนำข้อมูลออกจากระบบคอมพิวเตอร์
  - ✓ เป็นไปตามประกาศกระทรวงดิจิทัล

ม. 26 เก็บข้อมูลจราจรทางคอมพิวเตอร์

ประกาศ ทก. เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

(90 วัน ไม่เกิน 2 ปี) เป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

“ข้อมูลจราจรทางคอมพิวเตอร์” ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิด ของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

หลักฐานสำคัญในการหาตัวอาชญากร **ปรับไม่เกิน 500,000 บาท**

- ✓ เวลาต้องเที่ยงตรง เพื่อให้ระบุเส้นทางได้ถูก
- ✓ ข้อมูลจราจรทางคอมพิวเตอร์ที่เก็บต้องสามารถระบุตัวบุคคลได้
- ✓ ข้อมูลจราจรทางคอมพิวเตอร์ที่ต้องไม่ถูกแก้ไข

หากไม่เก็บจะทำให้ยากในการติดตามผู้กระทำความผิด และวิเคราะห์ข้อบกพร่องของระบบ

ม.18 การรวบรวมพยานหลักฐาน

- **เพิ่มเติม** พนักงานเจ้าหน้าทีซึ่งเชี่ยวชาญ ***ให้ช่วยเหลือทางเทคนิค*** แก่พนักงานสอบสวนตามกฎหมายอื่น *เงื่อนไข ต้องได้รับการร้องขอ จากพนักงานสอบสวน
- **ขอบเขต** ความผิดตาม พ.ร.บ. คอมฯ และ ผิดกฎหมายอื่นที่เกี่ยวข้อง
- **ผลที่ได้รับ** ประชาชน ***ได้รับการบรรเทาความเสียหาย*** อย่างเร็วที่สุด

1. เรียก Log File
2. สั่ง ISP ให้ส่งข้อมูล
3. ทำสำเนาข้อมูลจากคอมพิวเตอร์
4. **สั่งให้ส่งมอบข้อมูล/อุปกรณ์**
5. **ตรวจสอบ/เข้าถึง ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ log file**
6. **ถอดรหัสลับ**
7. **ยึด/อายัด ระบบคอมพิวเตอร์**

ต้องขอศาลก่อนดำเนินการ (ม.19)

ม. 20 การระงับการเผยแพร่ข้อมูล

- **เพิ่มเติม** ให้พนักงานสอบสวนร้องขอให้ ปิดเว็บไซต์ที่ **ผิดกฎหมายอื่น หรือ ขัดต่อความสงบ ได้**
- **ข้อมูลที่ระงับการเผยแพร่ได้ มีเฉพาะ**
  - ข้อมูลที่ผิดตาม พ.ร.บ. คอมฯ
  - ข้อมูลที่กระทบต่อความมั่นคงแห่งราชอาณาจักร ตาม ปอ.
  - ข้อมูลที่ผิดกฎหมาย IP
  - ข้อมูลคอมพิวเตอร์ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดี

เงื่อนไข : กรณี ข้อมูลคอมพิวเตอร์ขัดต่อความสงบเรียบร้อยและศีลธรรมอันดี ต้องผ่านการกลั่นกรองของคณะกรรมการกลั่นกรองฯ ก่อนเสนอต่อ รมว. และศาล เพื่อ **สร้างความสมดุล**

ขั้นตอนการออกคำสั่ง

1. กรณีขัดต่อกฎหมาย (คอม , ปอ. , IP)

พนักงานเจ้าหน้าที่ → รมว. → ศาล → **พนักงานเจ้าหน้าที่/ผู้ให้บริการ** ดำเนินการระงับ/ลบ

2. กรณีขัดต่อความสงบฯ

พนักงานเจ้าหน้าที่ → คณะกรรมการกลั่นกรอง → รมว. → ศาล → **พนักงานเจ้าหน้าที่/ผู้ให้บริการ** ดำเนินการระงับ/ลบ

ให้มีการ **ประกาศ/ระเบียบ** เพื่อให้เห็นแนวทางการใช้บังคับ

มาตรา 11 การส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์	• ประกาศ เรื่อง ลักษณะและวิธีการส่ง ลักษณะ และปริมาณของข้อมูล ความถี่แลวิธีการส่งซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ พ.ศ. 2560
มาตรา 15 ความรับผิดของผู้ให้บริการ	• ประกาศ เรื่อง ขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์และการนำข้อมูลคอมพิวเตอร์ออกจากระบบคอมพิวเตอร์ พ.ศ. 2560
มาตรา 17/1 คณะกรรมการเปรียบเทียบ	• ประกาศ เรื่อง แต่งตั้งคณะกรรมการเปรียบเทียบ ตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พ.ศ. 2560
มาตรา 20 การระงับการแพร่หลายข้อมูลคอมพิวเตอร์	• ประกาศ เรื่อง หลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือผู้ให้บริการ พ.ศ. 2560
มาตรา 20/1 การระงับการแพร่หลายข้อมูลคอมพิวเตอร์ที่ขัดต่อความสงบ	• ประกาศ เรื่อง แต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ ตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พ.ศ. 2560

ร่าง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

ร่าง พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

ดูแลเพื่อให้การใช้งานออนไลน์ปลอดภัย สร้างความเชื่อมั่นทางเศรษฐกิจ

- เพื่อป้องกัน และรับมือ
  พร้อมวิเคราะห์ แก้ไข/หยุดปัญหาให้เร็วที่สุด

- ปกป้อง CII ให้สามารถให้บริการได้อย่างต่อเนื่อง
  เช่น ISP โทรคมนาคม สาธารณูปโภค (ไฟฟ้า ประปา)
  ทำงานผ่าน Regulator เพื่อไม่ให้ทับซ้อนกันและบูรณาการการทำงานระหว่างกัน

*CII ย่อมาจาก Critical Information Infrastructure หรือโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

กว่าจะมาเป็นร่างกฎหมายไซเบอร์

ครม. อนุมัติ
หลักการร่าง
พ.ร.บ.
16 ม.ค. 2558

สคก.
Hearing ร่าง
11 มี.ค. 2558

สคก.
ขอทราบประเด็น
ประกอบการพิจารณา
19 ต.ค. 2559

ETDA
Hearing ร่าง
24 ม.ค. 2558

31 ต.ค. 2559
กระทรวงตั้ง
คกก. ทบทวน

28 พ.ย. 2559
สปท. เห็นชอบรายงาน
การศึกษาร่าง

สปท. เสนอรายงาน
ต่อ ครม.
21 ธ.ค. 2559

ธ.ค. 2559
กระทรวงแจ้งผล
ต่อ สคก.

8 ก.พ. 2560
แจ้งผลต่อ
หน่วยงานที่เกี่ยวข้อง

สปท. รายงาน
ความคืบหน้า ร่าง พ.ร.บ.
15 พ.ค. 2560

24 พ.ค. ถึง
7 มิ.ย. 2560
กระทรวง DE
Hearing ร่างผ่าน www.

มกราคม 2561
กระทรวง DE
ประชุมร่วมกับผู้เชี่ยวชาญ

8 – 25 มีนาคม 2561
กระทรวง DE
Hearing ร่าง ผ่าน www.

2 พ.ค. 2561
สคก. เริ่มต้น
พิจารณาร่าง

กันยายน 2561
สคก. พิจารณาร่างเสร็จ

26 ก.ย. 2561
ดศ. ยืนยันร่างที่ สคก.
ตรวจเสร็จต่อ สลค.
(หนังสือ ดศ. 0100.4/8852)

4 ต.ค. 2561
ดศ. ส่งเอกสารตาม
รธน. ม.77 ต่อ สลค.

4 ต.ค. 2561
ดศ. ส่งผลการ
พิจารณาคำขอตั้ง
หน่วยงานต่อ สลค.

กระทรวง DE Hearing
27 ก.ย. – 12 ต.ค. 2561

17 ต.ค. 2561
ดศ. ส่งเอกสารตาม
รธน. ม.77 เพิ่มเติม
ต่อ สลค.

ร่าง พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ....

วางโครงสร้างในการดูแล

- **คณะกรรมการระดับชาติ : ดูแลภาพรวมเชิงนโยบาย**
- **คณะกรรมการกำกับดูแล : เพื่อให้การทำงานตามนโยบายมีประสิทธิภาพ ติดตามและรับมือภัยคุกคาม กำหนดแนวการทำงานและมาตรฐานขั้นต่ำ**
- **คณะกรรมการบริหารสำนักงาน : ดูแลงานบริหารทั่วไปของสำนักงานที่เป็นศูนย์กลางในการประสานงานและเฝ้าระวังภัยคุกคาม**

CII มาจากไหน

คณะกรรมการ กำหนดกลุ่มภารกิจหรือบริการที่เป็น CII ปัจจุบัน ได้แก่

(1) ด้าน**ความมั่นคง**ของรัฐ
(2) ด้าน**บริการภาครัฐ**ที่สำคัญ
(3) ด้าน**การเงินการธนาคาร**
(4) ด้าน**เทคโนโลยีสารสนเทศและโทรคมนาคม**
(5) ด้านการ**ขนส่งและโลจิสติกส์**
(6) ด้าน**พลังงานและสาธารณูปโภค**
(7) ด้าน**สาธารณสุข**
(8) ด้านอื่นตามที่ กปช. ประกาศกำหนดเพิ่มเติม

กำหนด**ลักษณะหน่วยงาน**ที่มีภารกิจหรือการให้บริการที่เป็น CII

กรณี ไม่แน่ใจว่าเป็นหรือไม่เป็น CII พร้อมให้คณะกรรมการฯ ทบทวน

*CII ย่อมาจาก Critical Information Infrastructure หรือ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

การรับมือภัยคุกคามทางไซเบอร์
ของหน่วยงาน CII และหน่วยงานของรัฐ

1. คณะกรรมการกำหนดรายละเอียด
ภัยคุกคาม ๓ ระดับ
- เฝ้าระวัง
- ร้ายแรง
- วิกฤต

พร้อมแนวทางป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัย

2. เมื่อเกิดภัยคุกคามทางไซเบอร์

ให้หน่วยงานวิเคราะห์/ประเมิน ทำตามแผนรับมือ

3. **รายงานเหตุภัยคุกคามทางไซเบอร์**
ไปยัง Regulator และสำนักงาน ตามหลักเกณฑ์ที่คณะกรรมการกำหนด พร้อมขอความช่วยเหลือสำนักงานได้

4. **Regulator วิเคราะห์และประเมินสถานการณ์**
พร้อมให้ความช่วยเหลือ ทำงานร่วมกับสำนักงาน และแจ้งเตือนหน่วยงานใน Sector ของตน และ Regulator อื่น

5. **ในการรับมือภัยคุกคามระดับร้ายแรง เมื่อจำเป็น อาจต้องข้อมูลเชิงเทคนิค และให้ดำเนินการบางเรื่อง**
ทั้งให้เจ้าของระบบดำเนินการเอง หรือพนักงานเจ้าหน้าที่ดำเนินการ
หากภัยร้ายแรงและจำเป็นต้องเข้าถึงข้อมูล หรือยึดเครื่อง ต้องให้ศาลสั่งก่อนดำเนินการ

ขั้นวิกฤต หากเร่งด่วน ทำไปก่อน แล้วรายงานศาล

6. รายงานต่อคณะกรรการฯ อย่างต่อเนื่อง