



# ETDA MISSION



SECURITY | STANDARD | LAW  
—— e-COMMERCE ——

QUALITY OF LIFE & ECONOMIC GROWTH



# INCREASING VOLUME AND VALUE OF e-TRANSACTIONS

ETDA มุ่งพัฒนา

**SOFT INFRASTRUCTURE**

เพิ่มความเชื่อมั่นและอำนวยความสะดวก  
ในการทำธุรกรรมออนไลน์หรือ e-Transactions  
อันเป็นรากฐานสำคัญของ Digital Economy

e-COMMERCE  
PROMOTION

e-TRADE  
FACILITATION

SOFT  
INFRASTRUCTURE  
DEVELOPMENT

กำหนดมาตรฐาน ดูแลความมั่นคงปลอดภัยไซเบอร์  
และจัดทำกฎหมาย รองรับการทำธุรกรรมออนไลน์

**STANDARDS | SECURITY & PRIVACY | LAWS**



# e-TRANSACTIONS

# ENABLING AN ENVIRONMENT OF TRUST & CONFIDENCE IN e-TRANSACTIONS

## e-COMMERCE

- **SMEs Go Online**
  - ยกระดับการซื้อขาย & การให้บริการทางออนไลน์
  - ถ่ายทอดความรู้ & เคล็ดลับแบบมืออาชีพอย่างครบวงจร ทั้งสินค้าทั่วไป & Digital Contents
- **e-Directory “Thaيمarket.com”**
  - ทำระบบทะเบียนรองรับตัวตนของผู้ขาย & ผู้ให้บริการในโลกออนไลน์
  - สร้างความมั่นใจ ความมีตัวตน & มีอยู่จริงของ SMEs
  - Matching คู่ค้าทางธุรกิจ
- **OCC – Online Complaint Center**
  - เพิ่มช่องทางรับเรื่อง ช่วยแก้ไขปัญหา
  - เพื่อสนับสนุน Online Consumer Protection ให้แข็งแกร่ง
  - สายด่วน โทร.1212 หรือ 02-123-1223

## e-TRADE FACILITATION

- **e-Business & e-Trade**
  - พัฒนามาตรฐานข้อความที่เกี่ยวข้องกับการทำการค้า ได้แก่ e-Tax Invoice และ e-Receipt
- **ระบบการเชื่อมโยงข้อมูลอิเล็กทรอนิกส์ NSW**
  - ให้บริการลงทะเบียนรหัสสถานที่เพื่อการค้า & การขนส่ง (UN/LOCODE) เพื่อสนับสนุนกรมศุลกากร
- **NRCA (National Root CA)**
  - เป็นโครงสร้างพื้นฐาน รองรับการใช้ลายมือชื่อดิจิทัลและการเข้ารหัสลับ
- **e-Authentication Framework**
  - อำนวยความสะดวกในการทำธุรกรรมทางอิเล็กทรอนิกส์ข้ามพรมแดน
  - เตรียมความพร้อมเข้าสู่ AEC
  - กำหนดแนวปฏิบัติเกี่ยวกับการระบุตัวตนในโลกออนไลน์

## SOFT INFRASTRUCTURE

- **Policy & Statistics**
  - พัฒนาศาสตร์ศาสตร์รองรับ Soft Infrastructure (Standard, Security, Privacy & Laws)
  - จัดทำสถิติ & ดัชนีชี้วัด เพื่อให้มี baseline ที่สนับสนุนการทำธุรกรรมออนไลน์ของไทย
- **Digital Economy Laws**
  - พัฒนาและจัดทำกฎหมายรองรับธุรกรรมออนไลน์และนโยบายเศรษฐกิจดิจิทัล
  - จัดตั้ง ICT Law Center ศูนย์กลางกฎหมายไอซีทีหรือ DE Laws
  - จัด Open Forum ให้เป็นเวทีพูดคุยใน Topic สำคัญ ๆ & Hot Issues
- **e-Standards**
  - จัดทำมาตรฐานเชื่อมโยงข้อมูลหลังบ้าน เพื่อให้หน่วยงานและประชาชนได้รับบริการที่สะดวกรวดเร็ว รวมทั้งรองรับมาตรฐานที่ทำให้การค้าขายออนไลน์เติบโตมากขึ้น
- **Security & Privacy**
  - 1) **CERT Readiness ลดความเสี่ยง & ระบุภัยคุกคามทาง Online**
    - ฝึกระวัง แจ้งเตือนภัย ร่วมกับเครือข่าย CERT ทั่วโลก
    - จัดตั้ง Sector-based CERT ให้มีหน่วยที่ทำงานแบบ CERT ใน Sector ต่าง ๆ
  - 2) **Cybersecurity & Digital Forensics**
    - ทำดิจิทัลฟอเรนสิคส์ให้รู้ว่เกิดอะไรขึ้น จากไหน อย่างไร เพื่อลดความเสี่ยงทางออนไลน์และสนับสนุนงานบังคับใช้กฎหมาย
    - ผลักดันให้มีการใช้มาตรฐานเว็บไซต์ Website Security Standard & Secure Coding
    - พัฒนาวิชาชีพด้าน Cybersecurity & Digital Forensics



# OPPORTUNITIES AND TRENDS IN THAI E-COMMERCE ENVIRONMENT



## DIGITAL LIFESTYLE THAI POPULATION

Internet Users  
**27.65** MILLION

Source : TRUEHITS / 2014

Mobile  
Subscribers  
**97.68** MILLION

Source : NBTC / January 2015

Line Users  
**33** MILLION

Source : Tech in Asia; LINE / October 2014

Facebook Users  
**35** MILLION

Source : Zocialinc.com / April 2015

## e-PAYMENT 2014



**825,200**  
BILLION BAHT

Source : Bank of Thailand / 2014

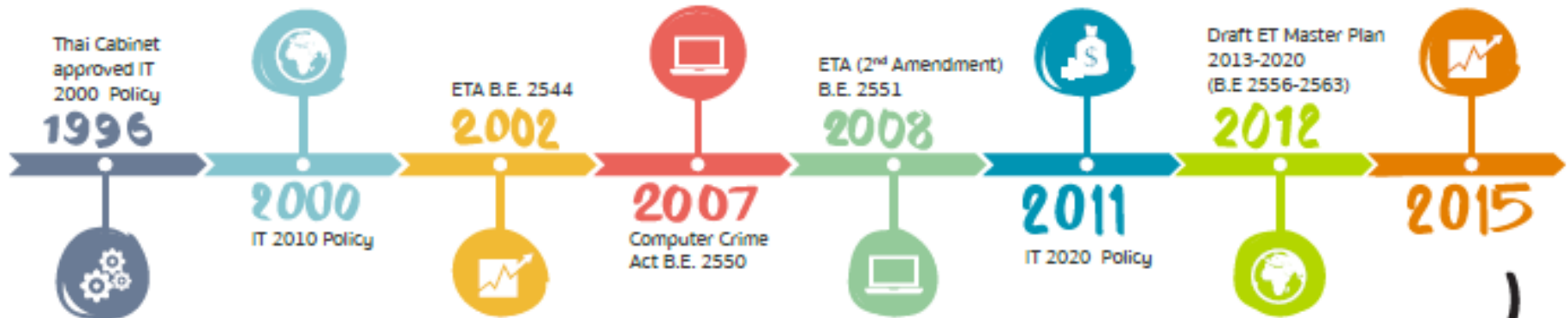
## e-COMMERCE 2014

**2,033.5**  
BILLION BAHT



Source : ETDA / 2014

# IT POLICY AND LEGAL DEVELOPMENT IN THAILAND



## DIGITAL ECONOMY LAW

CABINET APPROVED IN PRINCIPLE ON 18 DECEMBER 2014 AND 6 JANUARY 2015

ELECTRONIC TRANSACTIONS BILL (NO. ...) B.E. ... (NO. 3)

COMPUTER-RELATED CRIME BILL (NO. ...), B.E. ...

CYBER SECURITY PROTECTION BILL, B.E. ...

DATA PRIVACY BILL, B.E. ...

BILL ON ORGANIZATION OF MINISTRIES, SUB-MINISTRIES AND DEPARTMENTS (NO. ...), B.E. ...

BILL ON ORGANIZATION TO ASSIGN RADIO FREQUENCY AND TO REGULATE THE BROADCASTING AND TELECOMMUNICATIONS SERVICES (NO. ...), B.E. ...

BILL ON NATIONAL COMMITTEE FOR DIGITAL ECONOMY AND SOCIETY, B.E. ...

DIGITAL ECONOMY PROMOTION BILL, B.E. ...

DIGITAL DEVELOPMENT FUND FOR ECONOMY AND SOCIETY BILL, B.E. ...

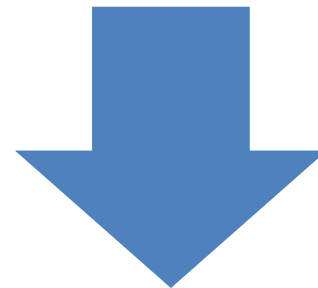
BUILDING TRUST

FUNDAMENTAL LAW



- เพิ่มความมั่นใจในการทำธุรกรรมออนไลน์
- สร้างความเท่าเทียมกับการทำในรูปแบบกระดาษ
- กลไกการยืนยันตัวตนบุคคล (Authentication)
- เพิ่มระบบความมั่นคงปลอดภัย (Security)
- เอาผิดผู้ก่ออาชญากรรมทางคอมพิวเตอร์
- คุ้มครองข้อมูลส่วนบุคคล

บทบาทของกฎหมาย IT



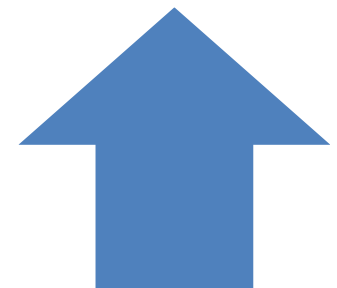
ควบคุม/เชิงรับ

เช่น พรบ.การกระทำความผิด  
เกี่ยวกับคอมพิวเตอร์, ร่างพรบ.  
ข้อมูลส่วนบุคคล



ส่งเสริม/เชิงรุก

เช่น พรบ.ธุรกรรมทาง  
อิเล็กทรอนิกส์ & กฎหมาย  
ลำดับรอง



# พัฒนาการกฎหมายธุรกรรมทางอิเล็กทรอนิกส์ของไทย

Model Law on  
Electronic  
Commerce

Model Law on  
Electronic  
Signatures

Transition Period  
Paper -> Electronic  
Electronic -> Paper

The United Nations  
Convention on the Use of  
Electronic Communications in  
International Contracts

พ.ร.บ.ว่าด้วยธุรกรรม  
ทางอิเล็กทรอนิกส์  
พ.ศ. 2544

กฎหมาย IT ฉบับแรกของไทย

พ.ร.บ.ว่าด้วยธุรกรรม  
ทางอิเล็กทรอนิกส์  
(ฉบับที่ 2) พ.ศ. 2551

พ.ร.บ.ว่าด้วยธุรกรรม  
ทางอิเล็กทรอนิกส์  
(ฉบับที่ ..) พ.ศ. ....

การพัฒนาในอนาคต

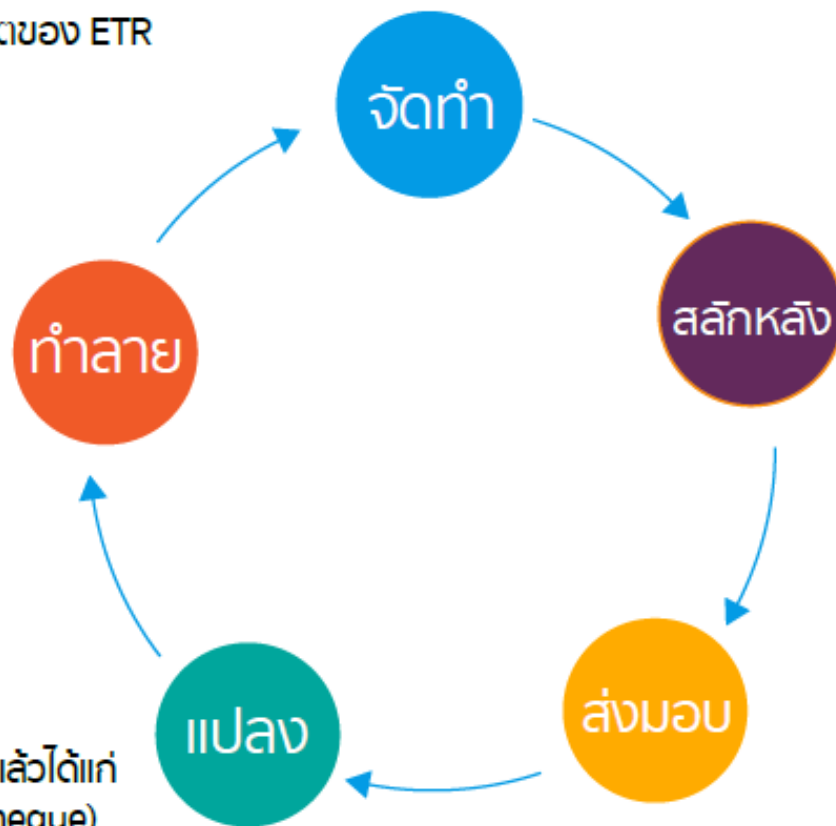
**Electronic  
Transferable  
Records**

**Online  
Dispute  
Resolution**

# [ e-Transferable Record (ETR) ]

เอกสารที่เปลี่ยนมือได้ทางอิเล็กทรอนิกส์

- UNCITRAL WG 4 กำลัง จัดทำ “ร่างหลักเกณฑ์รองรับ ETR” (เช่น Model Law) กำหนดให้ครบวงจรของชีวิตของ ETR ในระบบอิเล็กทรอนิกส์



- ปัจจุบัน ประเทศที่มีกฎหมายรองรับเรื่อง ETR แล้วได้แก่ เกาหลีใต้ (e-Promissory Note) ฮองกง (e-Cheque)



# การ Implement ระบบ e-Cheque ในฮ่องกง

## ระบบ e-Cheque ในฮ่องกง

 <b>Generic BANK</b>	11 08 2014 Day   Month   Year
Pay 香港银行同业结算有限公司 銀行	HONG KONG BANK 902911008
US Dollars TWO HUNDRED THOUSAND ONLY 美元	US\$ 200,000.00
HAPPY BUSINESS MAGAZINE PUBLISHING LTD.	Digitally signed by Mani Lee for and on behalf of HAPPY BUSINESS MAGAZINE PUBLISHING LTD. Date: 2014-07-16 16:17:10
123456 MA1 HSL 123456789	Digitally signed by Susan Wong for and on behalf of HAPPY BUSINESS MAGAZINE PUBLISHING LTD. Date: 2014-07-16 16:17:10
Remark 備註: Sample e-cheques by Citizon Limited	Prepared by Generic Bank Date: 2014-07-15 16:17:10



ต้นทุนการทำเช็ค  
กระดาษต่อใบ **17** HKD



วันทำงาน **250** วันต่อปี



มีเช็คในระบบ  
**500,000**  
ฉบับต่อวัน

\*\*ลดค่าใช้จ่ายได้กว่า 2 พันล้าน HKD ต่อปี

# องค์ประกอบของ e - Cheque

ใช้ digital signature เพื่อรับรองตัวตน และตรวจสอบความถูกต้อง

**Generic BANK** 11 08 2014  
Day 日 Month 月 Year 年

ชื่อผู้รับเงิน: 香港银行同业结算有限公司  
USD Dollars: TWO HUNDRED THOUSAND ONLY  
US\$ 200,000.00

ชื่อผู้ส่งจ่าย: HAPPY BUSINESS MAGAZINE PUBLISHING LTD.

หมายเหตุ: Sample e-cheques by Cerizen Limited

Account Payee Only

Digitally signed by Mary Lee for and on behalf of HAPPY BUSINESS MAGAZINE PUBLISHING LTD. Date: 2014-07-15 16:17:10

Digitally signed by Susan Wong for and on behalf of HAPPY BUSINESS MAGAZINE PUBLISHING LTD. Date: 2014-07-16 16:17:10

Prepared by Generic Bank Date: 2014-07-15 16:17:10

This is an e-cheque and is only regarded to be presented by sending the banker on which it is drawn in the form of an electronic record with a digital signature. We hereby expressly make presentation in any other manner and request our bank to make payment thereon against creation of the electronic record referred to above without requesting any other form of presentation under the title of Exchange Ordinance or otherwise.

Digital Certificate ของผู้ส่งจ่าย

KYC โดย CA

จัดเก็บใน Smart Card

Digital Certificate ของธนาคารผู้ส่งจ่าย

KYC โดยธนาคาร

จัดเก็บในอุปกรณ์ Hardware Security Module

# เปรียบเทียบกระบวนการสร้างเช็คในรูปแบบกระดาษและ e-Cheque

## e-Cheque      Paper Cheque

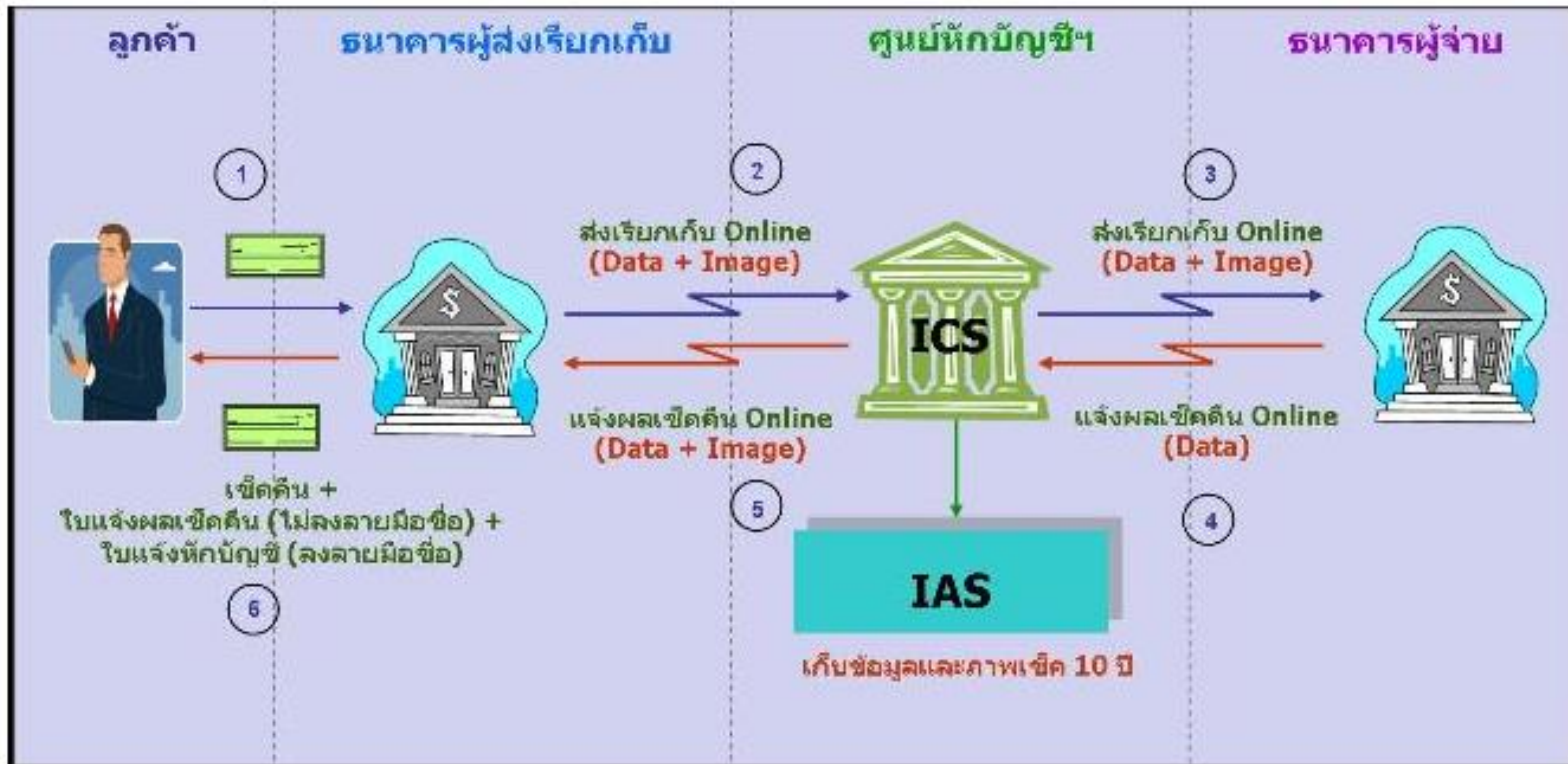
ผู้สั่งจ่ายกรอกแบบฟอร์ม      สร้าง e-Cheque ในรูปแบบไฟล์ PDF และสร้าง Digital Signature      สามารถส่งอีเมลไปยังผู้รับ      ผู้รับ Upload ไฟล์ e-Cheque เข้าสู่ระบบ



ผู้สั่งจ่ายกรอกเช็คกระดาษ      ลงนามกำกับ      ส่งเช็คให้ผู้รับโดยตรง      นำเช็คขึ้นเงินที่ธนาคาร

# ระบบการหักบัญชีเช็คและระบบการจัดเก็บภาพเช็ค

กระบวนการเรียกเก็บเงินตามเช็คในระบบ ICAS



ที่มา  
ธปท.

# DEVELOPMENT OF THAILAND ELECTRONIC TRANSACTIONS LAWS

PRINCIPLES

FUNCTIONAL EQUIVALENT APPROACH

TECHNOLOGY NEUTRALITY

PARTY AUTONOMY

MODEL LAWS



TO SUPPORT e-TRANSACTIONS



+

**ELECTRONIC TRANSACTIONS ACT B.E. 2544 & 2551**

**DRAFT OF ELECTRONIC TRANSACTIONS NO 3 ACT B.E. ....**

TO SUPPORT CROSS-BORDER e-TRANSACTIONS & AEC

1.

In conjunction with other laws,

2.

Legal effects,

3.

Admissibility of evidence in court

# หลักการพื้นฐานธุรกรรมทางอิเล็กทรอนิกส์

เท่าเทียมกระดาษ

Functional  
Equivalent  
Approach

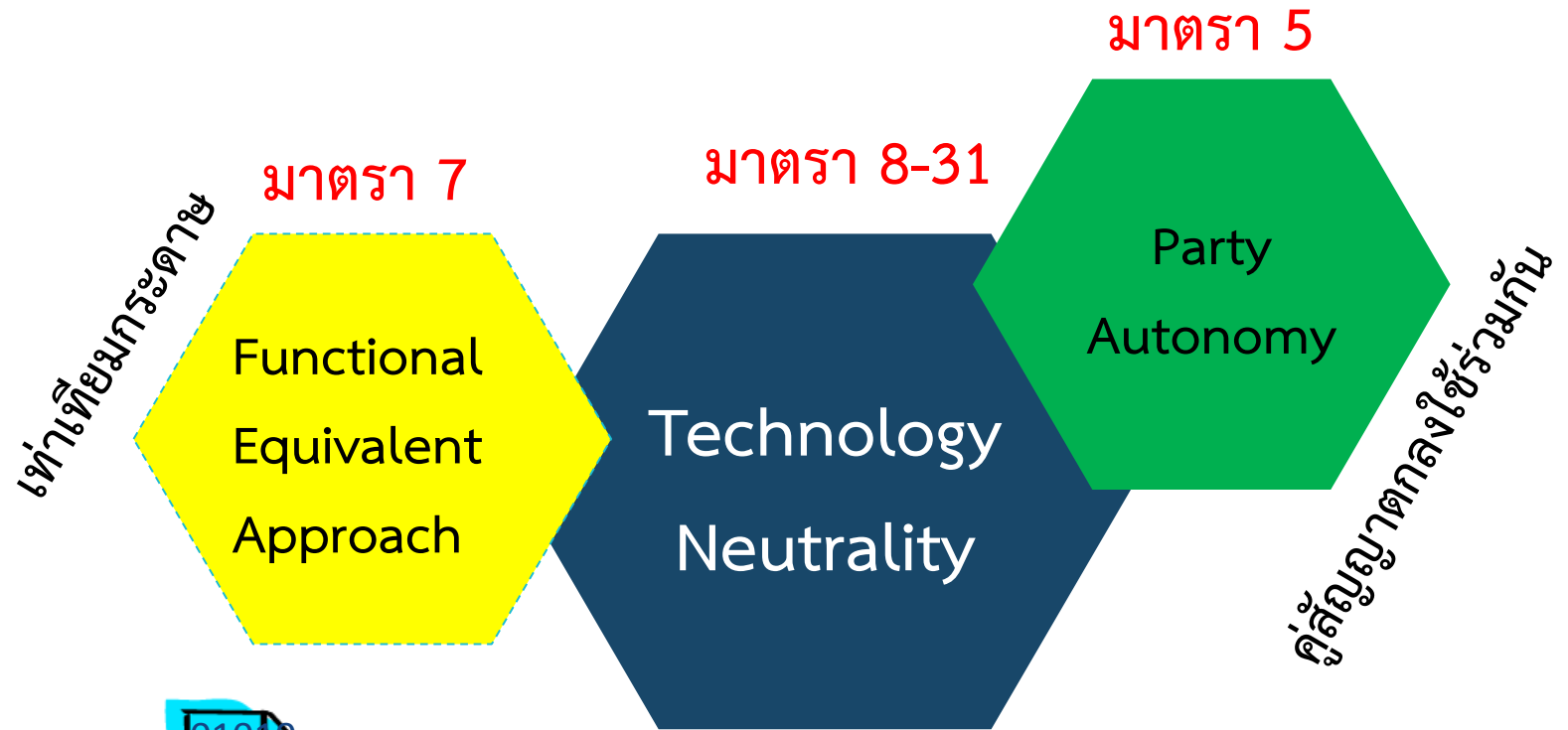
Technology  
Neutrality

Party  
Autonomy

คู่สัญญาตกลงใช้ร่วมกัน

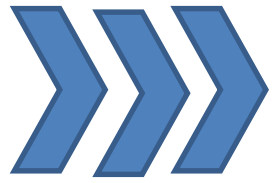
รองรับทุกเทคโนโลยี





รองรับทุกเทคโนโลยี





# ใช้บังคับเพื่อเสริมกฎหมายอื่น

(เสริมให้ทำในรูปแบบอิเล็กทรอนิกส์ได้)



พระราชบัญญัติว่าด้วย  
ธุรกรรมทางอิเล็กทรอนิกส์ฯ



ประมวลกฎหมายแพ่งและพาณิชย์  
(มาตรา 861 – 897)

รองรับให้ธุรกรรมกระดาษ  
ตามที่กำหนดในกฎหมายต่าง  
ๆ ทำในรูปแบบข้อมูล  
อิเล็กทรอนิกส์ได้

## ตัวอย่าง

สำนักงานคณะกรรมการกฤษฎีกา  
มาตรา ๘๖๗ อันสัญญาประกันภัยนั้น ถ้ามิได้มีหลักฐานเป็นหนังสืออย่างใด  
อย่างหนึ่งลงลายมือชื่อฝ่ายที่ต้องรับผิดชอบหรือลายมือชื่อตัวแทนของฝ่ายนั้นเป็นสำคัญ ท่านว่าจะ  
ฟ้องร้องให้บังคับคดีหาได้ไม่  
สำนักงานคณะกรรมการกฤษฎีกา  
ให้ส่งมอบกรมธรรม์ประกันภัยอันมีเนื้อความต้องตามสัญญานั้นแก่ผู้เอา  
ประกันภัยฉบับหนึ่ง  
สำนักงานคณะกรรมการกฤษฎีกา  
กรมธรรม์ประกันภัย ต้องลงลายมือชื่อของผู้รับประกันภัยและมีรายการตั้ง  
ต่อไปนี้  
สำนักงานคณะกรรมการกฤษฎีกา  
สำนักงานคณะกรรมการกฤษฎีกา



กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ไม่ใช้กับ (1) ธุรกรรมเกี่ยวกับครอบครัว  
(2) ธุรกรรมเกี่ยวกับมรดก



# ทำไมต้องรู้ว่าอะไรคือสิ่งที่กฎหมายกำหนด และอะไรเป็นขั้นตอนของเราเอง



## Law

ต้องปฏิบัติตาม

กฎหมายกำหนดแบบ ขั้นตอน เงื่อนไข อย่างไรบ้าง

(หากกฎหมายข้อไหนจะเป็นอุปสรรค/ไม่จำเป็นสำหรับ  
ระบบอิเล็กทรอนิกส์ **ต้องเสนอแก้ไขกฎหมาย**)



## Business Process

ปรับเปลี่ยนให้เหมาะสมกับ  
ระบบอิเล็กทรอนิกส์

ขั้นตอนภายในของเรากำหนด Business Process ไว้อย่างไร

(หากขั้นตอนไหนเป็นอุปสรรค/ไม่จำเป็นสำหรับระบบ  
อิเล็กทรอนิกส์ **เสนอผู้บริหารเพื่อปรับเปลี่ยนแก้ไข**)

# โครงสร้างกฎหมาย



## “ธุรกรรมทางอิเล็กทรอนิกส์”

รองรับการทำธุรกรรมในรูปแบบข้อมูลอิเล็กทรอนิกส์ในเรื่องต่างๆ

## “ลายมือชื่ออิเล็กทรอนิกส์”

รองรับลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

## “ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์”

รองรับการกำกับดูแลธุรกิจบริการที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ที่สำคัญและมีผลกระทบวงกว้าง

## “ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ”

รองรับการให้บริการภาครัฐด้วยวิธีการทางอิเล็กทรอนิกส์

## “คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์”

รองรับการมีคณะกรรมการเพื่อส่งเสริมและพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ

# Mandatory Rules

เมื่อตกลงใช้ธุรกรรมทางอิเล็กทรอนิกส์  
หลักเกณฑ์เหล่านี้ตกลงเป็นอย่างอื่นไม่ได้

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

หลักเกณฑ์อื่นนอกจากนี้  
ในหมวด 1 และ 2  
สามารถตกลงเป็นอย่างอื่นได้

# หลักเกณฑ์อื่น ๆ ที่ตกลงเป็นอย่างอื่นได้

- ม. 13 คำเสนอ / คำสนองในรูปแบบอิเล็กทรอนิกส์
- ม. 14 การแสดงเจตนา / บอกกล่าวในรูปแบบอิเล็กทรอนิกส์
- ม. 15 – ม. 21 การส่ง – รับ ข้อมูลอิเล็กทรอนิกส์
- ม. 22 มีการส่งข้อมูลอิเล็กทรอนิกส์เมื่อไหร่
- ม. 23 ได้รับข้อมูลอิเล็กทรอนิกส์เมื่อไหร่
- ม. 24 สถานที่ส่ง – รับ ข้อมูลอิเล็กทรอนิกส์คือที่ใด

สามารถตกลงร่วมกัน  
ในกลุ่มธุรกิจเพื่อให้  
เป็นมาตรฐานเดียวกัน  
ได้

# ELECTRONIC DOCUMENT

ม. 8

1.

เข้าถึงได้

2.

นำกลับมาใช้ได้

3.

ความหมายไม่  
เปลี่ยนแปลง



# SIGNATURE

ม. 9

1.

ระบุตัวผู้เป็นเจ้าของ  
ลายมือชื่อได้



2.

แสดงได้ว่าเจ้าของ  
ลายมือชื่อ  
ยอมรับข้อความนั้น



3.

ใช้วิธีการที่น่าเชื่อถือ



ความมั่นคงและรัดกุมของ  
วิธีการที่ใช้



ลักษณะ ประเภท หรือขนาด  
ของธุรกรรมที่ทำ ฯลฯ



ความรัดกุมของระบบ  
ติดต่อสื่อสาร

# SIGNATURE

## ม. 9

1.

ระบุตัวผู้เป็นเจ้าของลายมือชื่อได้

2.

แสดงได้ว่าเจ้าของลายมือชื่อยอมรับข้อความนั้น

3.

ใช้วิธีการที่น่าเชื่อถือ

## ม. 26

1.

ข้อมูลที่ใช้สร้างลายมือชื่อเชื่อมโยงไปยังเจ้าของได้

2.

ข้อมูลที่ใช้สร้างลายมือชื่ออยู่ภายใต้การควบคุมของเจ้าของ เมื่อสร้าง

3.

สามารถตรวจพบการเปลี่ยนแปลงของลายมือชื่อ / ข้อความ นับแต่สร้างได้

ลายมือชื่อที่เชื่อถือได้

# ตัวอย่างคำพิพากษาต่างประเทศ

## *Mehta v J Pereira Fernandes*

หากคู่สัญญาหรือตัวแทนของคู่สัญญาได้พิมพ์ชื่อหลักของตนไว้ท้ายอีเมล  
ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์

## *Golden Ocean Group Ltd v Salgaocar Mining Industries PVT Ltd* [2012] EWCA Civ 265

หากคู่สัญญาได้เขียนอีเมลหากันหรือลงลายมือชื่อถือว่าคู่สัญญาได้ผูกพันตาม  
ข้อความในอีเมลนั้น

อย่างไรก็ตามหากเป็นการพิมพ์ชื่อท้ายอีเมลและพิมพ์คำว่า “ตามสัญญา” (subject  
to contract) ถือว่า ข้อความหรือสัญญาที่ได้ตกลงในอีเมลไม่เป็นผลถึงแม้จะมีการ  
ลงลายมืออิเล็กทรอนิกส์ก็ตาม



# TRANSITION PERIOD

Paper → e-Doc  
←



ม. ๑๐ JSSA ๔

สิ่งพิมพ์ออก (printout)



ม. ๑๒

การแปลงเอกสารกระดาษเป็นเอกสารอิเล็กทรอนิกส์

อิเล็กทรอนิกส์ → กระดาษ

กระดาษ → อิเล็กทรอนิกส์



ม. ๑๑

ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์  
เป็นพยานหลักฐานในศาล

กฎหมายห้ามมิให้ปฏิเสธการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์  
(Admissibility of evidence in court)

แต่ การที่ศาลจะเชื่อถือในพยานหลักฐานทางอิเล็กทรอนิกส์หรือไม่ ขึ้นอยู่กับ



ความน่าเชื่อถือของพยานหลักฐาน

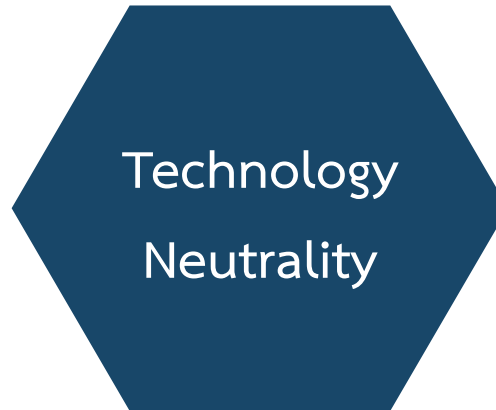


การชั่งน้ำหนักพยานหลักฐานของศาลเอง

# น่าเชื่อถือหรือไม่ ดูได้จากอะไร

- วิธีการที่ใช้ สอดคล้องตามเกณฑ์ที่กฎหมายกำหนดหรือไม่

มาตรา 8-31



- Standard ช่วยได้

# ● - EVIDENCE

ความน่าเชื่อถือของพยานหลักฐานดูจาก

ลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์

ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วนและไม่มีการเปลี่ยนแปลง

ลักษณะ วิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล

รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งหมด



มาตรา 25  
วิธีการแบบปลอดภัย

(การปฏิบัติตามมาตรา 25 จะได้ประโยชน์ จากข้อสันนิษฐานทางกฎหมาย)



# [ ทิศทางการพัฒนา e-Court ]

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

ประกาศราชกิจจานุเบกษาเมื่อ 8 ตุลาคม 2558

- รongรับการจัดทำสารบบความ สำนวนความในรูปแบบข้อมูลอิเล็กทรอนิกส์ รวมถึง Print out ของข้อมูลดังกล่าว
- รongรับการยื่นคำคู่ความและเอกสารในรูปแบบข้อมูลอิเล็กทรอนิกส์ เช่น ผ่านอีเมล



พระราชบัญญัติ

แก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง (ฉบับที่ ๒๘)  
พ.ศ. ๒๕๕๘

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑ ตุลาคม พ.ศ. ๒๕๕๘  
เป็นปีที่ ๘๖ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภาผู้แทนราษฎรในวาระที่ ๒๘ มีเนื้อ

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง (ฉบับที่ ๒๘) พ.ศ. ๒๕๕๘"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้ใช้ความต่อไปนี้เป็นมาตรา ๖/๑ แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง "มาตรา ๖/๑ คดีที่ขึ้นฟ้องหรือคำขอขึ้นบังคับใช้คำแพ่ง ก่อนวันขึ้นฟ้อง หรือก่อนวันขึ้นบังคับใช้คำขอขึ้นบังคับใช้คำแพ่งที่มีการฟ้องหรือคำขอขึ้นบังคับใช้คำแพ่งแล้วแต่ยังมิได้ยื่นคำขอขึ้นบังคับใช้คำแพ่งหรือการนำฎีกาหรือการขอรวมคดีหรือยื่นคำขอโอนการคุ้มครองผู้ไม่ตกเป็นส่วรวม หรือประโยชน์สาธารณะอย่างอื่นที่มีสำคัญ และการโอนคดีไปยังศาลแห่งอื่น จะให้การพิจารณาคดีเป็นไปอย่างมีประสิทธิภาพยิ่งขึ้น ก็ให้ศาลเจ้าคู่ความและทนายความเห็นชอบก่อนศาลอุทธรณ์เห็นชอบก่อนศาลต้นฟ้องคดีนั้นก็ได้" คำสั่งของประธานศาลอุทธรณ์ให้เป็นที่สุด

# ตัวอย่างการรับฟังข้อมูลอิเล็กทรอนิกส์ เป็นพยานหลักฐาน

ฎีกาที่ 8089/2556

✓ การเบิกถอนเงินสดจากบัญชีเงินฝากผ่านตู้ ATM  
เป็นธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งรับฟังได้ตามมาตรา 7

✓ การนำบัตรกดเงินสดไปถอนเงินและใส่รหัสส่วนตัว เสมือนการลงลายมือชื่อตนเอง  
ซึ่งถือเป็นการลงลายมือชื่ออิเล็กทรอนิกส์ตามมาตรา 9

✓ เมื่อจำเลยนำบัตรกดเงินสดไปถอนเงิน ใส่รหัสเพื่อทำรายการถอนเงิน และ  
กดยืนยันทำรายการ พร้อมรับเงินสดและสลิป การกระทำดังกล่าวจึงถือเป็น  
หลักฐานการกู้ยืมเงิน ตามมาตรา 8 วรรคหนึ่ง

# พยานหลักฐานอะไรที่ใช้สืบในคดีที่เกิดใน Internet

ต้องสืบอย่างไรศาลจึงจะรับฟัง

“Digital Forensic”

## ฎีกายกฟ้อง คดี 112 'เบนโตะ' โพสต์บอร์ดประชาไท ชี้ แค่เลข IP address บ่งชี้ไม่ได้

Tue, 2015-10-20 14:29

หลังจากเมื่อวันที่ 11 ก.ย. ที่ผ่านมา ศาลอาญา รัชดา ได้นัดฟังคำพิพากษาศาลฎีกา คดีนพวรรณ หรือ เบนโตะ ผู้โพสต์ในเว็บบอร์ดประชาไทปี 51 แต่เนื่องจากจำเลยไม่มาศาล โดยนายประกันระบุว่าไม่สามารถติดต่อจำเลยได้ ศาลจึงอนุมัติหมายจับ เพื่อนำตัวมาฟังคำพิพากษา พร้อมเลื่อนฟังคำพิพากษามาวันนี้ (20 ต.ค. 58) ซึ่ง [โครงการอินเทอร์เน็ตเพื่อกฎหมายประชาชน \(iLaw\)](#) รายงานว่า ศาลอ่านคำพิพากษาศาลฎีกาคดีดังกล่าวสรุปความว่า "ตัวเลข IP address บ่งชี้ไม่ได้ว่าจำเลยมีความเกี่ยวข้องกับข้อความที่โพสต์และพยานโจทก์ก็มีความสงสัยตลอดมา ศาลจึงฎีกาจำเลยกลับ ให้ยกฟ้อง

โดย [ประชาชาติธุรกิจ](#) รายงานคำพิพากษาว่า ศาลฎีกาพิเคราะห์จากคำเบิกความของโจทก์ แล้วเห็นว่าไม่สอดคล้องกัน ซึ่งนางสาวนพวรรณ ก็ให้การปฏิเสธ มาโดยตลอด จึงยกประโยชน์แห่งความสงสัยให้จำเลย ศาลฎีกาพิพากษากลับยกฟ้อง

รู้ยัง ? IP ADDRESS คืออะไร

# การยกระดับความมั่นคงปลอดภัย และความน่าเชื่อถือของการทำธุรกรรม

## ทางอิเล็กทรอนิกส์สำหรับธุรกิจประกันภัย

มาตรา 25 แห่ง พ.ร.บ.

ธุรกรรมฯ

+

พ.ร.ฎ.ว่าด้วยวิธีการแบบ

ปลอดภัยในการทำ

ธุรกรรมทาง

อิเล็กทรอนิกส์ พ.ศ.

2553



เป็นการรักษาความมั่นคงปลอดภัย ให้มีการยอมรับและเชื่อมั่น  
ในข้อมูลอิเล็กทรอนิกส์เพิ่มมากยิ่งขึ้น

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ  
ตามวิธีการแบบปลอดภัย ปฏิบัติได้ดังนี้

- การสร้างความมั่นคงปลอดภัยด้านการบริหารจัดการและระบบสารสนเทศ
- การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์หรือควบคุมการเข้าถึงข้อมูลอิเล็กทรอนิกส์
- การบริหารจัดการด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์และไม่อาจคาดคิด
- การบริหารจัดการด้านบริการให้มีความต่อเนื่องเป็นต้น

ผล

เมื่อปฏิบัติตามวิธีการแบบปลอดภัยตามระดับของตนแล้ว  
จะได้ประโยชน์จากข้อสันนิษฐานของกฎหมาย  
ว่าได้ใช้วิธีการที่น่าเชื่อถือแล้ว



การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบมั่นคงปลอดภัย  
(ประกาศ คธอ. เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของ  
ธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555)

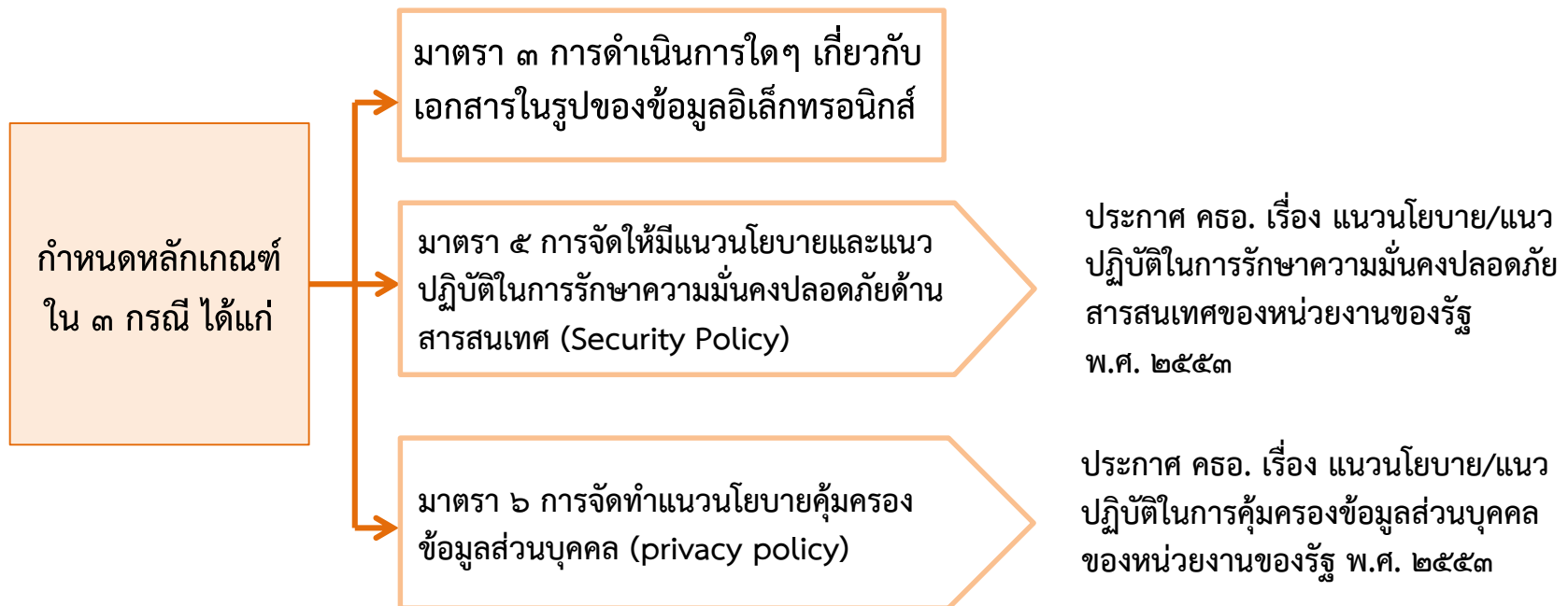
การประเมินระดับผลกระทบ ที่เกิดขึ้นใน 1 วัน	<b>Security Basic</b> ผลกระทบระดับต่ำ	<b>Security Medium</b> ผลกระทบระดับกลาง	<b>Security High Level</b> ผลกระทบระดับสูง
(1) ผลกระทบด้านมูลค่าความเสียหาย ทางการเงิน	≤ 1 ล้านบาท	≥ 1 ล้านบาท ≤ 100 ล้านบาท	≥ 100 ล้านบาท
(2) ผลกระทบต่อจำนวนผู้ใช้บริการหรือ ผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างกายหรือนามัย	ไม่มีผู้ใช้บริการได้รับผลกระทบ ต่อชีวิต ร่างกาย หรืออนามัย	ผู้ใช้บริการได้รับผลกระทบ ต่อร่างกาย หรืออนามัย ≥ 1 คน ≤ 1,000 คน	ผู้ใช้บริการได้รับผลกระทบ ต่อร่างกายหรืออนามัย ≥ 1,000 คน หรือต่อชีวิต ตั้งแต่ 1 คน
(3) ผลกระทบต่อจำนวนผู้ใช้บริการหรือ ผู้มีส่วนได้เสียที่อาจได้รับความเสียหาย อื่นใดนอกจาก (2)	ผู้ใช้บริการได้รับผลกระทบ ≤ 10,000 คน	ผู้ใช้บริการได้รับผลกระทบ ≥ 10,000 คน แต่ ≤ 100,000 คน	ผู้ใช้บริการได้รับผลกระทบ ≥ 100,000 คน
(4) ผลกระทบด้านความมั่นคงของรัฐ	<u>ไม่มี</u> ผลกระทบต่อความมั่นคง ของรัฐ	-	<u>มี</u> ผลกระทบต่อความมั่นคง ของรัฐ
		หากมีผลกระทบระดับกลางอย่าง น้อย 2 ด้านขึ้นไปให้ใช้วิธีการแบบ ปลอดภัยในระดับกลางขึ้นไป	หากมีผลกระทบระดับสูงเพียง 1 ด้านต้องใช้วิธีการแบบมั่นคง ปลอดภัยในระดับเคร่งครัด

# พ.ร.ฎ.กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

พ.ศ. ๒๕๕๙

## “หน่วยงานของรัฐ” ตาม พ.ร.บ.ธุรกรรมฯ มาตรา ๔

- กระทรวง ทบวง กรม ส่วนราชการ ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น
- รัฐวิสาหกิจที่ตั้งขึ้นโดย พ.ร.บ. หรือ พ.ร.ฎ.
- นิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในการใดๆ



# ความท้าทายด้าน Cyber-security และ Privacy

## Cybersecurity has been rising continuously.

### Cybercrime is rising significantly in Europe

Europe dominates over other regions in detecting security incidents, reporting a **41% jump** over 2013.

### Incidents are more costly to large organisations

Organisations reporting financial hits of \$20 million or more increased 92% over 2013.

Global security incidents (GSISS 2015)

48%

Global smartphone users (eMarketer)

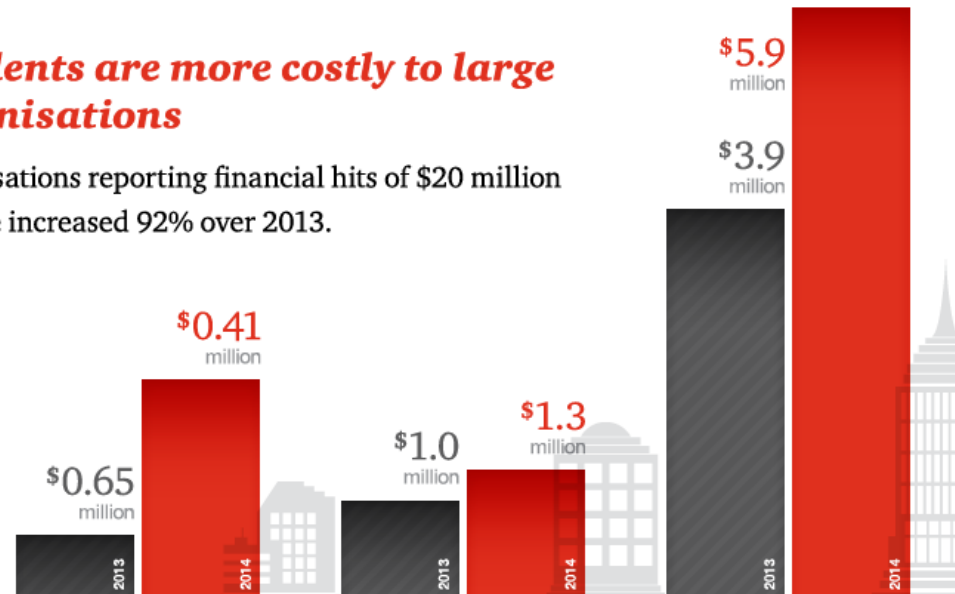
22%

Global GDP (OECD)

21%

### Security incidents outpace GDP and mobile phone growth

The percentage of growth for global security incidents is **more than double** global GDP and global smartphone users combined.



Global State of Information

Security Survey 2015 By PWC

 **REUTERS** 2014

## JPMorgan hack exposed data of 83 million, among biggest breaches in history

the largest theft of customer data from a U.S. financial institution.

 **The Washington Post** 2015

## Hackers just stole data on 15 million T-Mobile customers

Hackers got the names, addresses, Social Security numbers, and identification numbers.

 **ABC** 2015

## VTech data hack: Private details of 5m parents stolen from popular electronic toy maker

Hackers have stolen the private details of nearly 5 million people.

 **theguardian** 2015

## US government hack stole fingerprints of 5.6 million federal employees

Some 20 million people had their name, home address, and Social Security number stolen. 5.6 million fingerprints were also taken.

# News

## From 2014-2016

 **BBC** 2015

## Sony Pictures computer system hacked in online attack

 **CBR** 2015  
Computer Business Review

## Ukrainian power grid cyberattack reveals widely used Trojan malware

The incident left the town, Ivano-Frankivsk, without electricity for several hours.

 **NBC NEWS** 2016

## Time Warner Warns Customers Their Emails and Passwords May Have Been Stolen

by DEVIN COLDEWEY

320,000 customers may have had their emails and passwords leaked.

# 2015 Cost and Impact of Data Breaches by EUROSTAFF

## Cost and Impact of

# Data Breaches

"The number of companies using and relying on technology to manage data is increasing - so too are the numbers of those wishing to steal that information."



JP Morgan Chase (2014)  
**Cost - \$250 Million**  
  
 Users affected - 80 Million  
 Source: ibtimes.com

Target (2014)  
**Cost - \$148 Million**  
  
 Users affected - 100 Million  
 Source: nytimes.com

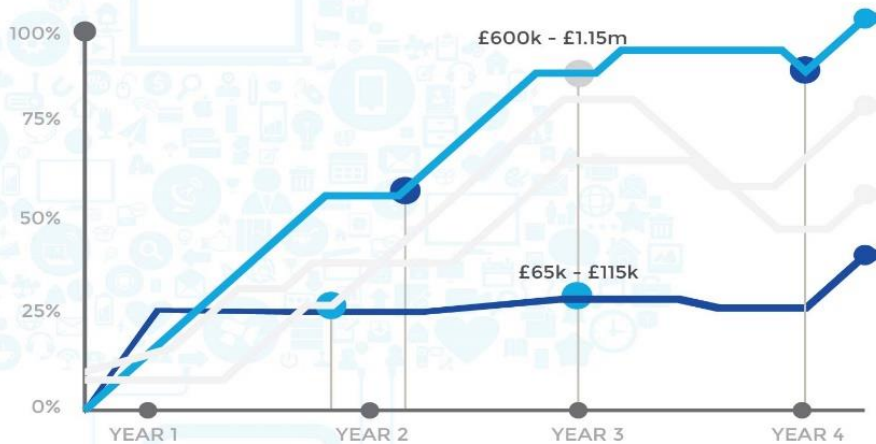
Home Depot (2015)  
**Cost - \$53 Million**  
  
 Users affected - 56 Million  
 Source: esecurityplanet.com

Zappos (2012)  
**Cost - \$106,000**  
  
 Users affected - 24 million  
 Source: internetretailer.com

Sony (2014)  
**Cost - \$170 Million**  
  
 Users affected - 24.6 Million  
 Source: tomsguide.com

Ebay (2014)  
**Cost - \$18 Million**  
  
 Users affected - 145 Million  
 Source: scmagazineuk.com

## The cost of a Data Breach



Source: www.pwc.co.uk

**£1.46m - £3.14m**

The average cost of a data breach to a large organisation - up from £600k - £1.15m last year

**£75k - £311k**

The average cost of a data breach to a small business - up from £65k - £115k last year

# 2014

## BREACH LEVEL INDEX

### THE NUMBERS

RECORDS BREACHED IN 2014

**1,023,108,267**

NUMBER OF BREACH INCIDENTS

**1,541**

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

EVERY DAY  
2,803,036

EVERY HOUR  
116,793

EVERY MINUTE  
1,947

EVERY SECOND  
32

# 2015

## First Half Review

Findings from the  
**BREACH LEVEL INDEX**

POWERED BY

**gemalto**  
security to be free

### BREACH LEVEL INDEX

### THE NUMBERS

“ More and more organizations are accepting the fact that, despite their best efforts, security breaches are unavoidable. ”

RECORDS BREACHED IN FIRST HALF OF 2015

# 245,919,393

NUMBER OF BREACH INCIDENTS

# 888

TOP 10 BREACHES  
PERCENTAGE OF TOTAL RECORDS

# 82%

PERCENTAGE OF BREACHES  
WHERE NUMBER OF COMPROMISED  
RECORDS WAS UNKNOWN

# 50%

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

EVERY  
DAY  
1,358,671

EVERY  
HOUR  
56,611

EVERY  
MINUTE  
943

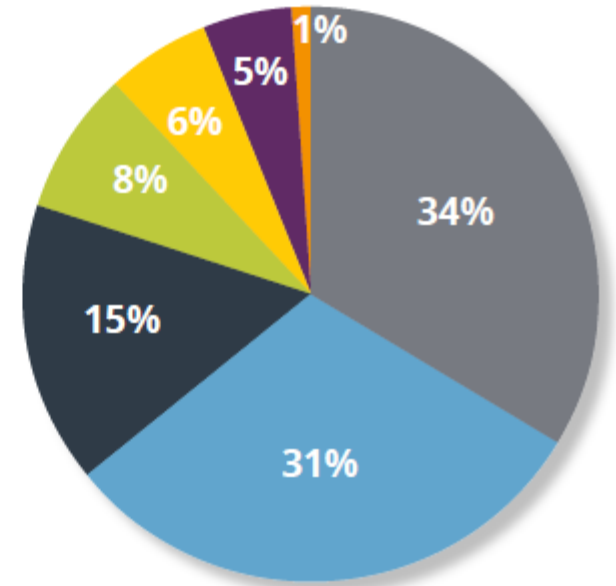
EVERY  
SECOND  
16

# 2015 First Half Review

Findings from the  
**BREACH LEVEL INDEX**

POWERED BY

**gemalto**  
security to be free



## NUMBER OF BREACH INCIDENTS BY INDUSTRY OVER TIME

INDUSTRY	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015
Healthcare	172	168	236	200	186
Financial Services	79	87	85	125	143
Government	128	65	108	182	142
Retail	58	42	83	112	115
Education	7	26	88	84	94
Technology	56	54	72	65	47
Other Industries	151	113	142	131	161

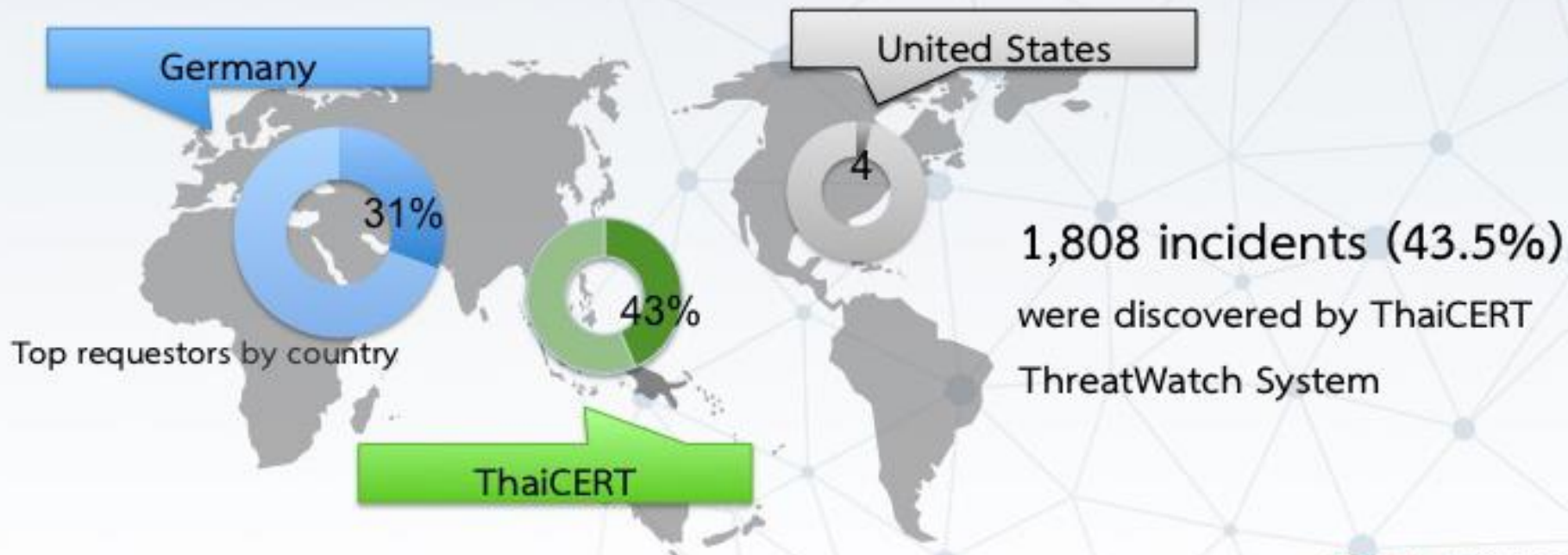


# สถิติภัยคุกคามไซเบอร์ในปี 2558

ThaiCERT handled  
4,157 incidents.

- Malicious code 1,496 (36%)
- Fraud (Phishing) 1,066 (25.6%)
- Intrusion 950 (22.9%)

Report by Incident Type



# Cybersecurity Trend

USA

## Cybersecurity



Protecting the Nation's economic prosperity, national security and our individual liberties by securing cyberspace

- Information sharing
- Limit liability
- Data breach notification
- Enforce criminal penalties

On January 14, President Obama came to the NCCIC and announced his Administration's support for more cybersecurity legislation

## Cybersecurity Legislation In USA

DHS 2015 : The Secretary's Progress Report

The Need for Cybersecurity  
Legislation

## Cybersecurity

- National Cybersecurity Protection Act of 2014  
(codifies the authority of DHS to assist the private sector)
- Federal Information Security Management Act of 2014  
(codifies authority of DHS to assist other federal agencies)
- Border Patrol Agent Pay Reform Act of 2014  
(ensures DHS's ability to hire and pay cybersecurity workforce)



Homeland  
Security

# กลยุทธ์หลักในการจัดการปัญหาความมั่นคงปลอดภัยไซเบอร์

## ยกร่างกฎหมายและจัดทำนโยบาย

- ▶ ยกร่างพรบ. ความมั่นคงปลอดภัยไซเบอร์ และกรอบนโยบายความมั่นคงปลอดภัยไซเบอร์

## ศูนย์ประสานการรับมือภัยคุกคาม

- ▶ สร้างความเข้มแข็งให้ไทยเซิร์ต และส่งเสริมให้หน่วยงานของรัฐและเอกชนตั้ง CERT [ระบบบริหารจัดการ เช่น ticketing, email, web] [ระบบวิเคราะห์ เช่น malware, vulnerability]

## ทำงานกับผู้มีส่วนได้เสีย

- ▶ พัฒนา Incident Handling Flow กับหน่วยงานสำคัญ เช่น หน่วยงานในกลุ่มธนาคาร หน่วยงานในกลุ่มบังคับใช้กฎหมาย

## เตรียมความพร้อมและเฝ้าระวัง

- ▶ จัดอบรม จัดแข่งขัน ช้อมรับมือภัยคุกคาม จัดทำมาตรฐาน และ Standard Operating Procedure (SOP) [ระบบ Government Monitoring System]

# ความท้าทายด้าน Cybersecurity และ Privacy

## เหตุการณ์ที่พบทั่วโลก

### สืบเนื่องจาก IoT, cloud

- หน้าเว็บถูกเปลี่ยน
- ข้อมูลถูกเจาะและนำไปเผยแพร่/ขาย
- ฉ้อโกงโดยใช้อีเมล
- ใช้มัลแวร์ขโมยข้อมูล\*



## แนวทางการดูแลระดับประเทศ

- กำหนดนโยบายและแผนที่ชัดเจน
- มีคณะกรรมการและหน่วยงานรับผิดชอบเชิงนโยบายและปฏิบัติ
- มีการบริหารจัดการก่อน ระหว่าง และหลังเกิดเหตุ
- มีหลักเกณฑ์การบริหารจัดการที่ยอมรับได้
- มีบทกำหนดโทษที่เหมาะสม

### (ร่าง) พรบ. คุ้มครองข้อมูลส่วนบุคคล

- กำหนดให้คำนิยามกลางของ “ข้อมูลส่วนบุคคล” เจ้าของข้อมูล และผู้ดูแลข้อมูล รวมถึงสิทธิและหน้าที่ที่เกี่ยวข้อง
- กำหนดหลักเกณฑ์ในการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลที่สอดคล้องกับแนวทางสากล
- กำหนดกลไกการดูแลข้อมูลทั้งแบบรัฐ และ เอกชน แบบ Self-regulation

### (ร่าง) พรบ. ความมั่นคงปลอดภัยไซเบอร์

- กลไกการวางนโยบายไซเบอร์ที่มี alignment ระหว่างหน่วยงาน
- แผนปฏิบัติ แผนรับมือ และ command center ที่สอดคล้องกับระดับของภัยคุกคาม
- หน่วยงานกลางเพื่อประเมินสถานการณ์ ประสานงาน และพร้อมรับมือภัยคุกคาม 24 ชั่วโมง
- อาศัยความร่วมมือจากรัฐ และ เอกชน ครอบคลุม การดูแลแบบ Self-regulation

\* มัลแวร์หรือ malware มาจาก malicious software หรือซอฟต์แวร์ประสงค์ร้ายที่มักจะมีพฤติกรรมขโมยข้อมูลในระบบคอมพิวเตอร์ หรือ smart phone

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

สภาพปัญหา	การละเมิด privacy รุนแรงมากขึ้น เช่น IoT, Cloud, Big Data	
ความจำเป็นในการ ตรากฎหมาย	กำหนดมาตรการคุ้มครองที่เพียงพอและเหมาะสม	
	ข้อกำหนดในเวทีระดับประเทศมีอิทธิพลต่อไทย	OECD / <b>EU Directive (Supra-national)</b> UN / APEC / Privacy Commissioner
	กฎหมายในประเทศมีอยู่บ้าง แต่ไม่ครบ และ บางส่วนแย้งกันเอง (ขาดกฎหมายกลาง)	ขาดมาตรการการคุ้มครองที่เหมาะสม
สาระสำคัญ	Privacy (Personal Information) คืออะไร?	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคล นั้นได้ไม่ว่า “ทางตรง” หรือ “ทางอ้อม”
	ผู้ที่เกี่ยวข้องมีใครบ้าง? เจ้าของข้อมูล (Data Subject) ผู้ควบคุมข้อมูล (Data Controller)	ก่อให้เกิดสิทธิและหน้าที่ต่อกัน
	กระบวนการที่เกี่ยวข้องกับข้อมูล?	เก็บ ใช้ เปิดเผย ดูแลให้มั่นคงปลอดภัย (ในประเทศ/ต่างประเทศ)
	ใครดูแล?	รัฐ หรือ เอกชนผ่าน Self-Regulation (ไทยให้ความสำคัญทั้งสองบทบาท)

# สาระสำคัญของร่างพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ....

## เป็นกฎหมายกลางใช้เป็นการทั่วไป

- ยกเว้นกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต เป็นต้น

## คุ้มครองอย่างเหมาะสมทุกขั้นตอน

- ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลในทุกขั้นตอนทั้งการเก็บรวบรวม ใช้ และเปิดเผย

## การส่งผ่านข้อมูลระหว่างประเทศที่มีความยืดหยุ่น

- สอดคล้อง APEC Cross Border Privacy Rules System

## พิจารณาข้อร้องเรียนที่มีประสิทธิภาพและรวดเร็ว

- พิจารณาข้อร้องเรียนโดยคณะกรรมการผู้เชี่ยวชาญโดยเฉพาะ
- กำหนดมาตรการไกล่เกลี่ยและเปรียบเทียบปรับ

## คุ้มครองข้อมูลส่วนบุคคลเทียบเท่าระดับสากล

- นำหลักการสากล OECD Guidelines และ APEC Privacy Framework มาบัญญัติไว้อย่างครบถ้วน

## มาตรการส่งเสริมการ Self regulation

- กำหนดมาตรการส่งเสริมและสร้างความตระหนักในการคุ้มครอง เช่น
- นโยบายการคุ้มครองความเป็นส่วนตัว (Privacy Policy)
  - เครื่องหมายรับรองมาตรฐาน (Trust Mark)
  - หน่วยงานรับรองตรวจสอบความโปร่งใส (Accountability Agent)

## หน่วยงานกำกับดูแลมีความรู้ความเชี่ยวชาญเฉพาะ

- ให้สำนักงานความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีความรู้เฉพาะด้าน (technical expertise) ทั้งด้านคุ้มครองข้อมูลส่วนบุคคล (Privacy) ความมั่นคงปลอดภัย (Cybersecurity) และมาตรฐาน (Standard)

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

สภาพปัญหา	ภัยคุกคามไซเบอร์รุนแรงมากขึ้นเรื่อยๆ
	ระบบอ่อนแอ หน่วยงานส่วนใหญ่ไม่สนใจ IT Security
ความจำเป็นในการตรากฎหมาย	เพื่อให้มีกลไกที่ประสานการทำงานร่วมกันในเชิงรุก เพื่อรับมือและแก้ปัญหาอย่างรวดเร็ว การคุกคามทางออนไลน์ที่กระทบเศรษฐกิจในภาพรวม และเป็น linkage ที่ทำงานร่วมกับฝั่งความมั่นคงด้วยความรวดเร็ว
	การจำกัดขอบเขตความเสียหายทำได้ยาก จึงต้องมีความรวดเร็วและความร่วมมือในการจัดการ
สาระสำคัญ	<p>Policy Level :</p> <ul style="list-style-type: none"><li>• วางนโยบายด้านไซเบอร์ ซึ่งเป็นภาพรวมของประเทศเพื่อสร้างความเข้มแข็งของระบบในทุกด้าน</li></ul> <p>คณะกรรมการนโยบาย</p> <p>Action Plan :</p> <ul style="list-style-type: none"><li>• จัดระดับภัยคุกคามและผลกระทบ</li><li>• มีแผนปฏิบัติงาน และแผนรับมือ</li><li>• มุ่งเน้นการดูแลเหตุที่ส่งผลกระทบต่อเศรษฐกิจและสังคม</li><li>• Command Center ยามเกิดเหตุร้ายแรง</li></ul> <p>แผนปฏิบัติการ และ National Flow</p> <p>Implementation :</p> <ul style="list-style-type: none"><li>• มีศูนย์กลางข้อมูล เพื่อรวบรวมข้อมูล วิเคราะห์ ประเมินสถานการณ์</li><li>• ประสานงานทุกส่วน และบุคลากรพร้อมรับมือ 24 ชั่วโมง</li></ul> <p>หน่วยงานกลาง</p> <p>Stakeholder</p> <ul style="list-style-type: none"><li>• อาศัยความร่วมมือจากทุกภาคส่วนในการรวบรวมข้อมูล</li><li>• Self-Regulation</li><li>• สร้างความตระหนัก ส่งเสริมความรู้ในการใช้งานทุกระดับ</li></ul>

การดำเนินการในบางกรณีอาจกระทบต่อสิทธิ/เสรีภาพของบุคคล จึงต้องพิจารณามาตรการอย่างรอบคอบ และต้องได้สมดุลระหว่างการรักษาความมั่นคงปลอดภัย & สิทธิของประชาชน โดยอยู่บนพื้นฐานของหลักสากล

(Legality / Necessity / Proportionality / Legitimacy / Nationality / Non-Discrimination)

- **ก่อนเกิดเหตุ**

- จัดทำ Policy / Guideline สำหรับให้หน่วยงานปฏิบัติในการดูแลรักษาระบบสารสนเทศตามมาตรฐานและเป็นไปในทิศทางเดียวกัน
- กำหนด Action plan และ Incident response (กำหนดระดับความร้ายแรง และการดำเนินการเมื่อเกิดเหตุ)
- ติดตาม ดูแล ให้หน่วยงานปฏิบัติตาม Policy / guideline อย่างสม่ำเสมอ
- ฝ้าระวัง และแจ้งเตือนเหตุภัยคุกคาม

- **ระหว่างเกิดเหตุ**

- ปฏิบัติการจัดการเหตุภัยคุกคามตามระดับความร้ายแรง -- กำหนดระดับความร้ายแรง
- จัดการ / แก้ไข / ระงับเหตุ ในกรณีฉุกเฉิน

- **หลังเกิดเหตุ**

- รวบรวมข้อมูลเพื่อนำมาวิเคราะห์และทบทวน/ปรับปรุงแผนรับมืออย่างสม่ำเสมอ



# พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

## บททั่วไป

## หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์

## หมวด 2 พนักงานเจ้าหน้าที่

- ระบบคอมพิวเตอร์
- ข้อมูลคอมพิวเตอร์
- ข้อมูลจราจรทาง คอมพิวเตอร์
- ผู้ให้บริการ
- ผู้ใช้บริการ
- พนักงานเจ้าหน้าที่
- รัฐมนตรี

### กระทำต่อคอมพิวเตอร์

- ม.5 การเข้าถึงระบบคอมพิวเตอร์
- ม.6 การล่วงรู้มาตรการการป้องกันการเข้าถึง
- ม.7 การเข้าถึงข้อมูลคอมพิวเตอร์
- ม.8 การดักจับข้อมูลคอมพิวเตอร์
- ม.9 การรบกวนข้อมูลคอมพิวเตอร์
- ม.10 การรบกวนระบบคอมพิวเตอร์
- ม.13 การจำหน่าย/ เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด

### ใช้คอมพิวเตอร์กระทำความผิด

- ม.11 Spam mail
- ม.14 การปลอมแปลงข้อมูลคอมพิวเตอร์/เผยแพร่เนื้อหาอันไม่เหมาะสม
- ม.15 ความรับผิดของผู้ให้บริการ
- ม.16 การเผยแพร่ภาพจากการติดต่อ/ตัดแปลง

### พนักงานเจ้าหน้าที่

**อำนาจหน้าที่ (ม.18) :** (1) มีหนังสือ/เรียกเพื่อให้ ถ้อยคำ/เอกสาร (2) เรียกข้อมูลจราจร (3) สั่งให้ ส่งมอบข้อมูลที่อยู่ในครอบครอง (4) ทำสำเนา ข้อมูล (5) สั่งให้ส่งมอบข้อมูล/อุปกรณ์ (6) ตรวจสอบ/เข้าถึง (7) ถอดรหัสลับ (8) ยึด/อายัด ระบบ

**ข้อจำกัด/การตรวจสอบการใช้อำนาจ (ม.19) :** ยื่นคำร้องต่อศาลในการใช้อำนาจตาม ม.18 (4)-(8), ส่งสำเนานับที่รายละเอียดให้แก่ศาลภายใน 48 ชม., ยึด/อายัดห้ามเกิน 30 วัน ขอยกยัดได้อีก 60 วัน (ม.18(8))

**การ block เว็บไซต์ พนักงานเจ้าหน้าที่โดยความเห็นชอบของรมว.ทก.ยื่นคำร้องต่อศาล (ม.20)**

**ความรับผิดของพนักงานเจ้าหน้าที่: (ม.22 ถึง มาตรา 24)**

**พยานหลักฐานที่ได้มาโดยมิชอบ อ้างและรับฟังมิได้ (ม.25)**

**การแต่งตั้ง/กำหนดคุณสมบัติพนักงานเจ้าหน้าที่/การประสานงาน (ม.28-29)**

### ผู้ให้บริการ

**ม.26** เก็บข้อมูลจราจร 90 วัน ไม่เกิน 1 ปี

**ม.27:** ไม่ปฏิบัติตามคำสั่งพนักงานเจ้าหน้าที่หรือคำสั่งศาล ระวังโทษปรับ

**กระทำความผิดนอกราชอาณาจักร ต้องรับโทษภายในราชอาณาจักร (ม.17)**

**การรับฟังพยานหลักฐานที่ได้มาตาม พ.ร.บ.ฉบับนี้ (ม.25)**

# กฎหมายลำดับรองที่ออกภายใต้

## พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ม.19 แบบหนังสือแสดงการยึดหรืออายัด  
ระบบคอมพิวเตอร์



กฎกระทรวงกำหนดแบบหนังสือแสดงการยึด  
หรืออายัดระบบคอมพิวเตอร์ พ.ศ 2551

ม.26 หน้าที่ของผู้ให้บริการในการเก็บรักษา  
ข้อมูลจราจรทางคอมพิวเตอร์



ประกาศ ทก. เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูล  
จราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

ม.28 คุณสมบัติของพนักงานเจ้าหน้าที่



ประกาศ ทก. เรื่อง หลักเกณฑ์เกี่ยวกับการกำหนด  
คุณสมบัติของพนักงานเจ้าหน้าที่ฯ

ม.29 อำนาจพนักงานเจ้าหน้าที่



ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวน  
สอบสวนและดำเนินคดีกับผู้กระทำความผิด  
ตาม พ.ร.บ.คอมฯ พ.ศ. 2550

ม.30 บัตรประจำตัวของพนักงานเจ้าหน้าที่



ประกาศ ทก. เรื่อง กำหนดแบบบัตรประจำตัว  
พนักงานเจ้าหน้าที่ฯ

THANK YOU

