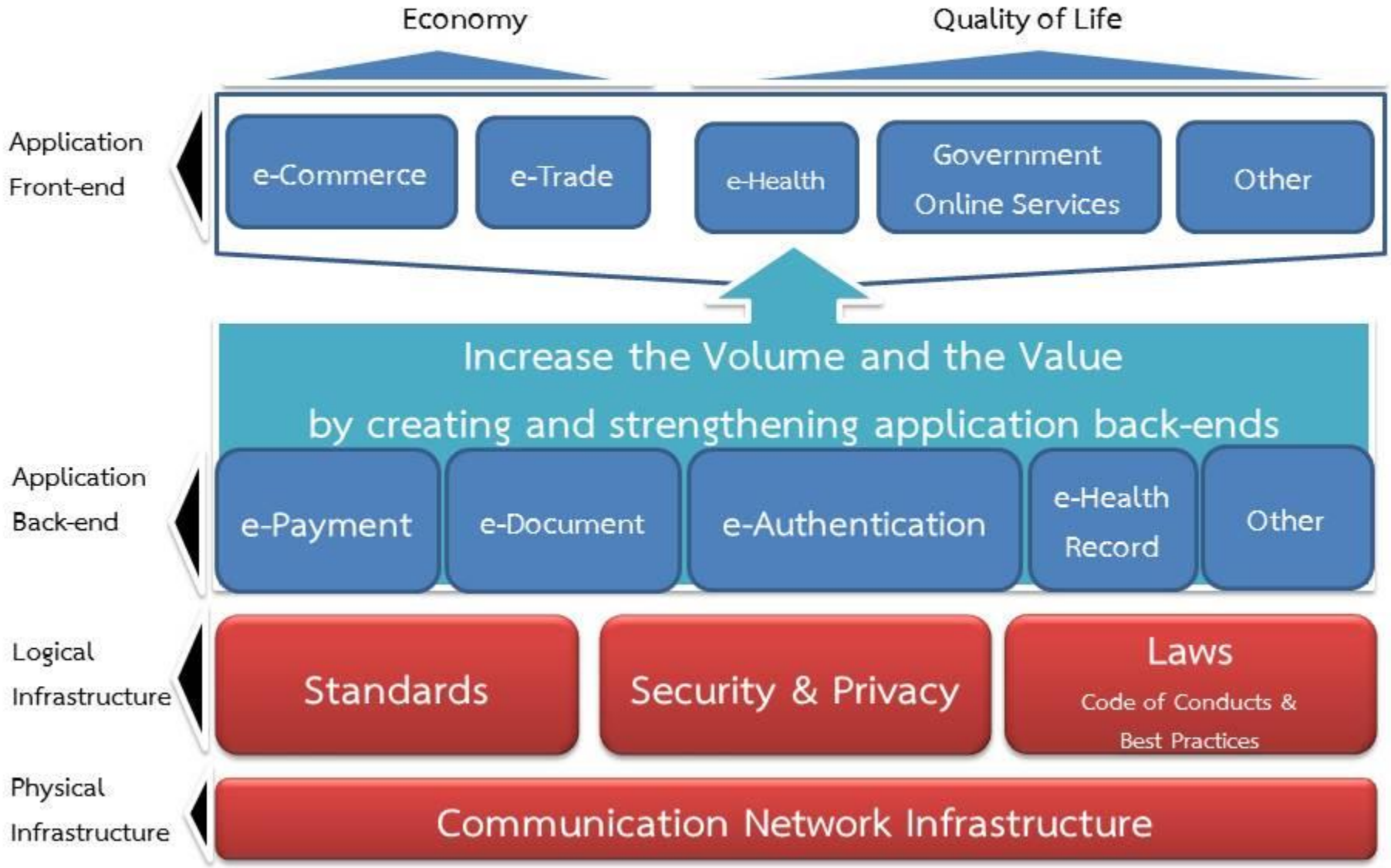
ETDA MISSION

SECURITY | STANDARD | LAW

e-COMMERCE

QUALITY OF LIFE & ECONOMIC GROWTH

Secure e-Transactions Development



ETDA
www.etda.or.th

ข้อมูลการใช้งานอินเทอร์เน็ตในบุคคลทั่วไป

- สำรวจเดือนเม.ย.-พ.ค. 57
- เข้ามาตอบด้วยความสมัครใจ (Self-selection)
- มีผู้ตอบ 16,596 คน

รักแท้แพ้ระยะทาง

สมาร์ตโฟน

77.1% ใช้เข้าถึงอินเทอร์เน็ต
ใช้งานเฉลี่ย 6.6 ชั่วโมงต่อวัน

คอมพิวเตอร์ตั้งโต๊ะ

69.4% ใช้เข้าถึงอินเทอร์เน็ต
ใช้งานเฉลี่ย 6.2 ชั่วโมงต่อวัน

คอมพิวเตอร์พกพา

49.5% ใช้เข้าถึงอินเทอร์เน็ต
ใช้งานเฉลี่ย 5.3 ชั่วโมงต่อวัน

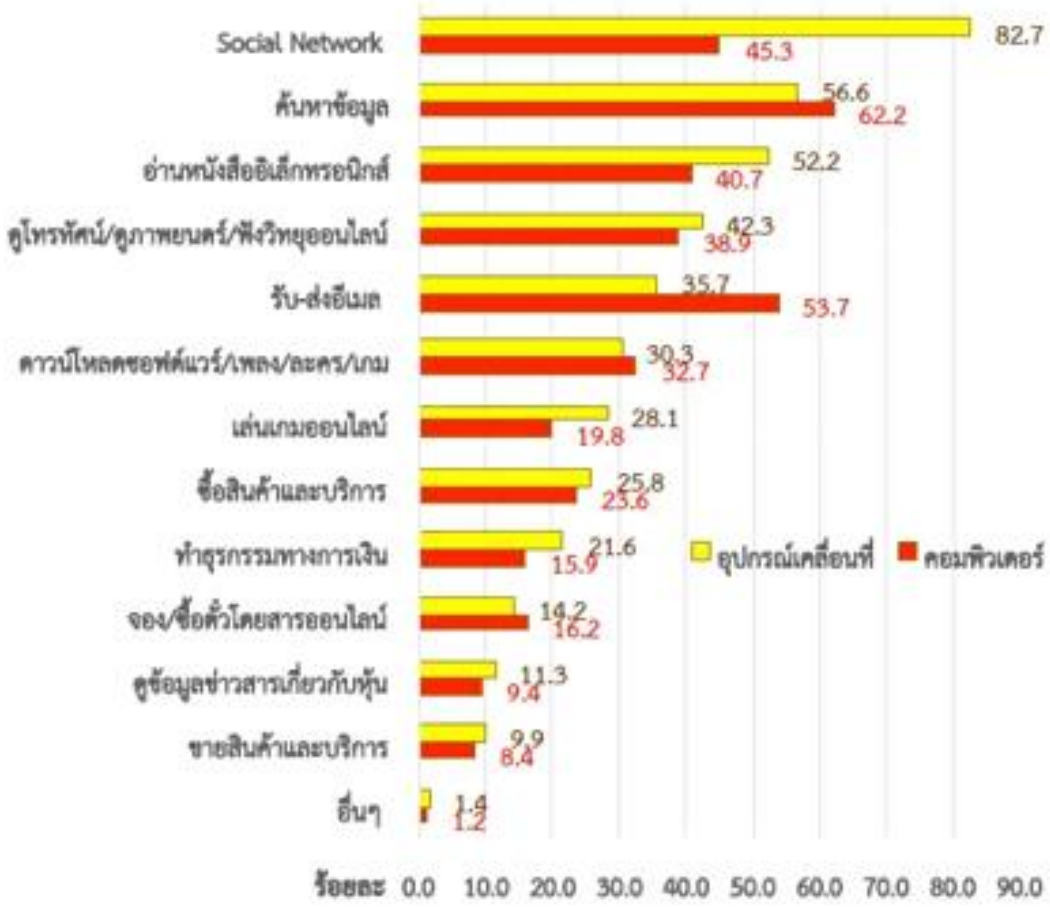
แท็บเล็ตคอมพิวเตอร์

31.1% ใช้เข้าถึงอินเทอร์เน็ต
ใช้งานเฉลี่ย 4.8 ชั่วโมงต่อวัน

สมาร์ตทีวี

8.4% ใช้เข้าถึงอินเทอร์เน็ต
ใช้งานเฉลี่ย 3.4 ชั่วโมงต่อวัน

Thailand Internet User Profile 2015



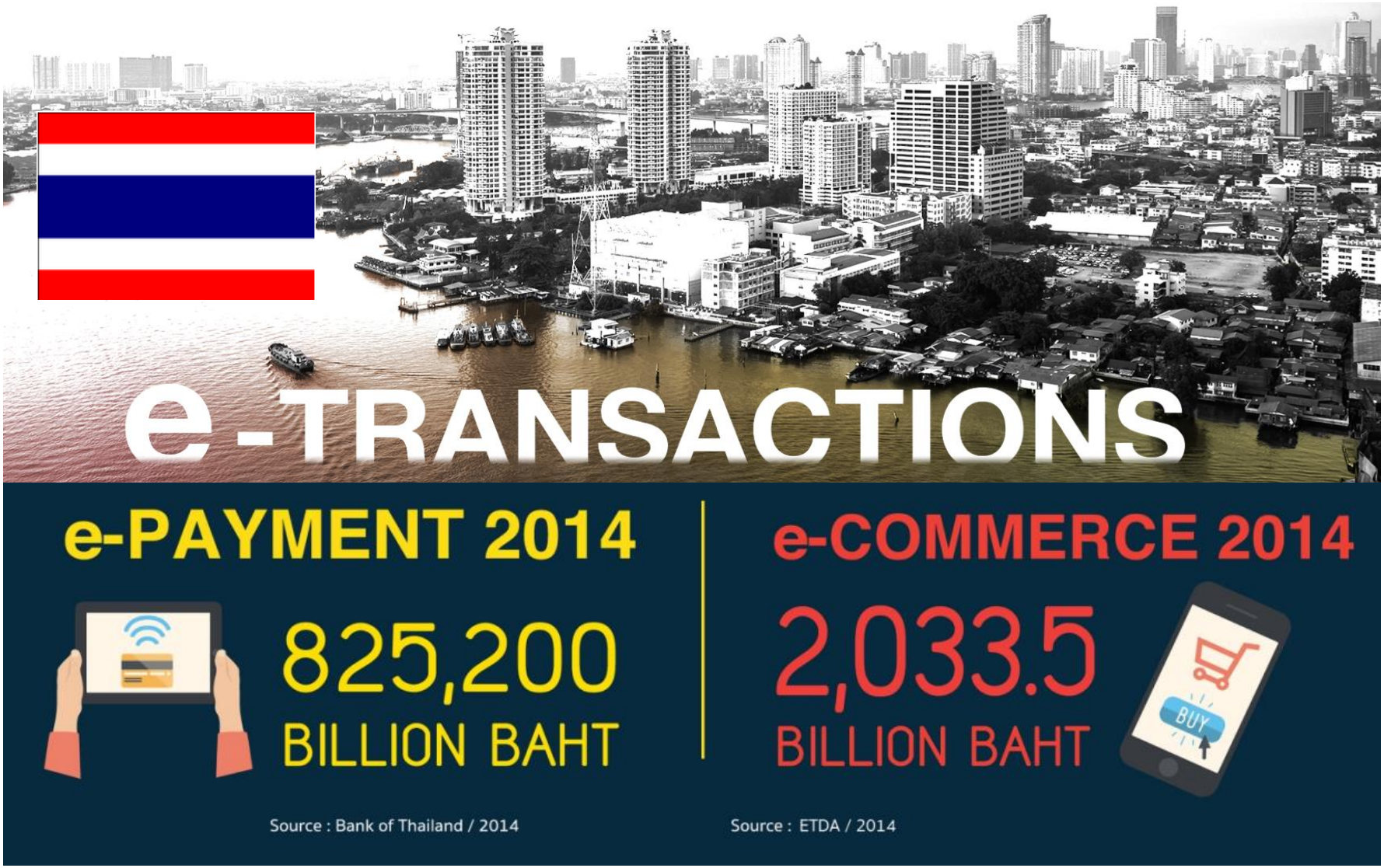
กิจกรรมยอดฮิต (สำหรับ Mobile Devices)

1. เครือข่ายสังคมออนไลน์
2. ค้นหาขอ้มูล
3. อ่าน e-News, e-Book

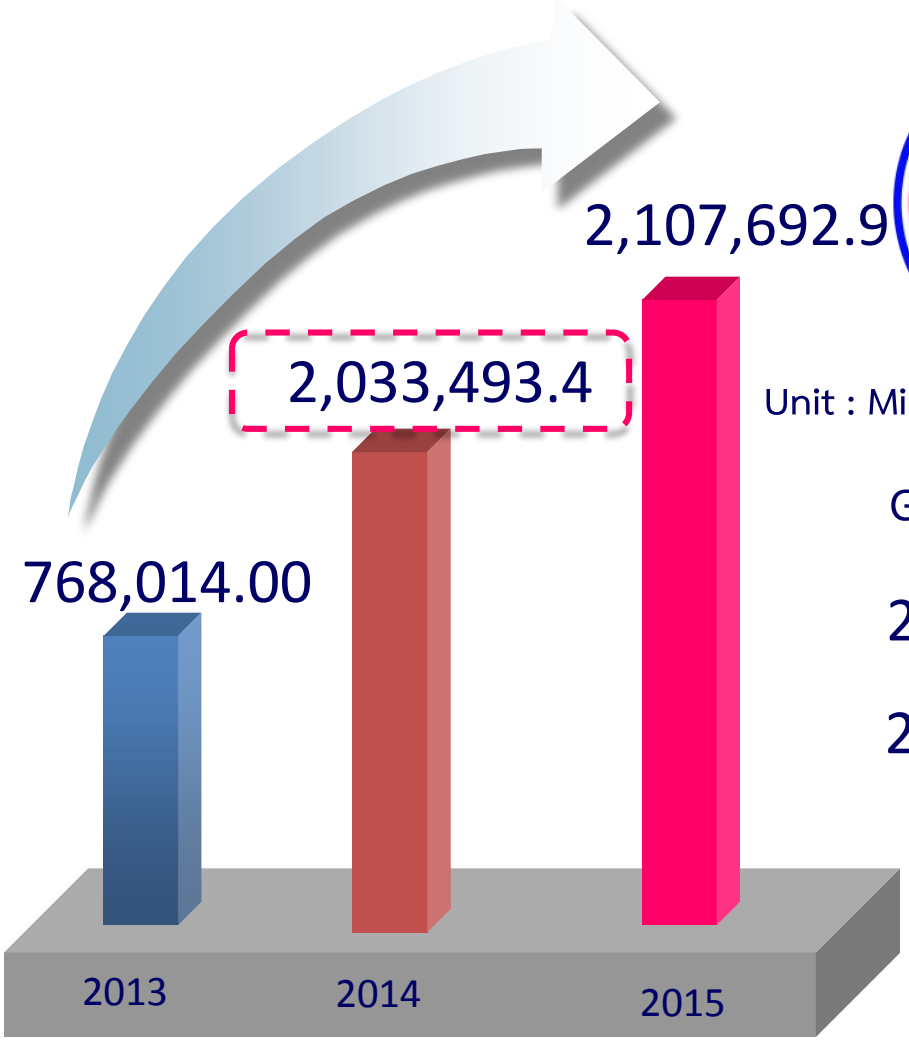
กิจกรรมยอดฮิต (สำหรับ คอมพิวเตอร์)

1. ค้นหาข้อมูล
2. รับ-ส่งอีเมล
3. เครือข่ายสังคมออนไลน์

สถิติ E-Commerce ไทย



Value of e-Commerce in Thailand 2013-2015



Unit : Million Baht

Growth Rate

2014 164.77%

2015 3.65%

Remarks :

2013 surveyed by National Statistical Office of Thailand

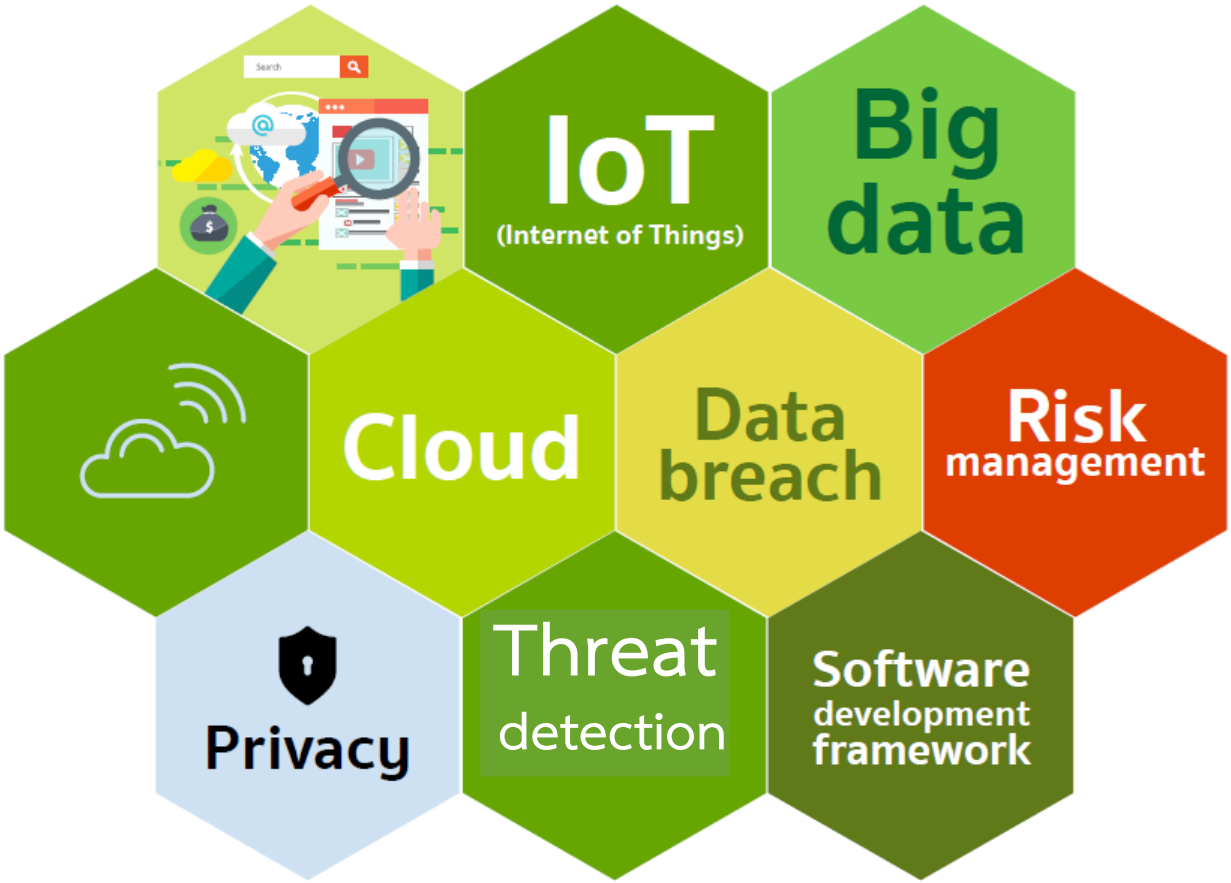
2014-2015 surveyed by ETDA

Value of e-Commerce

Source : ETDA, The Survey of Value of e-Commerce in Thailand, 2015

RSA Conference 2015

Popular Topics



INTERNET OF THINGS

BY 2020, THERE WILL BE
50 BILLION DEVICES (CISCO'S PREDICTION)

YOUR **UNDERWEAR**
IS THE INTERNET DEVICES THAT CAN MONITOR YOUR WEIGHT AND DIRECTLY ORDER THE FOOD AT THE RESTAURANT TO MATCH WITH YOUR WEIGHT AND HEALTH STATUS.

สถิติภัยคุกคามไซเบอร์ในปี 2558

ThaiCERT handled 4,371 incidents

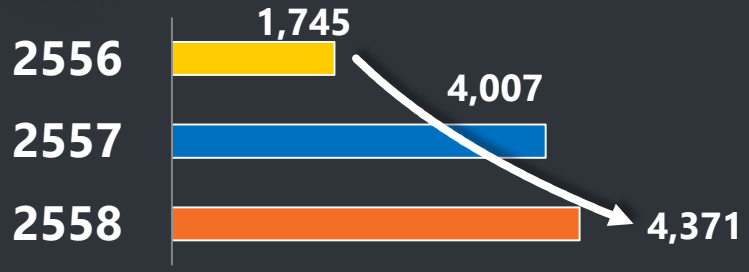
ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

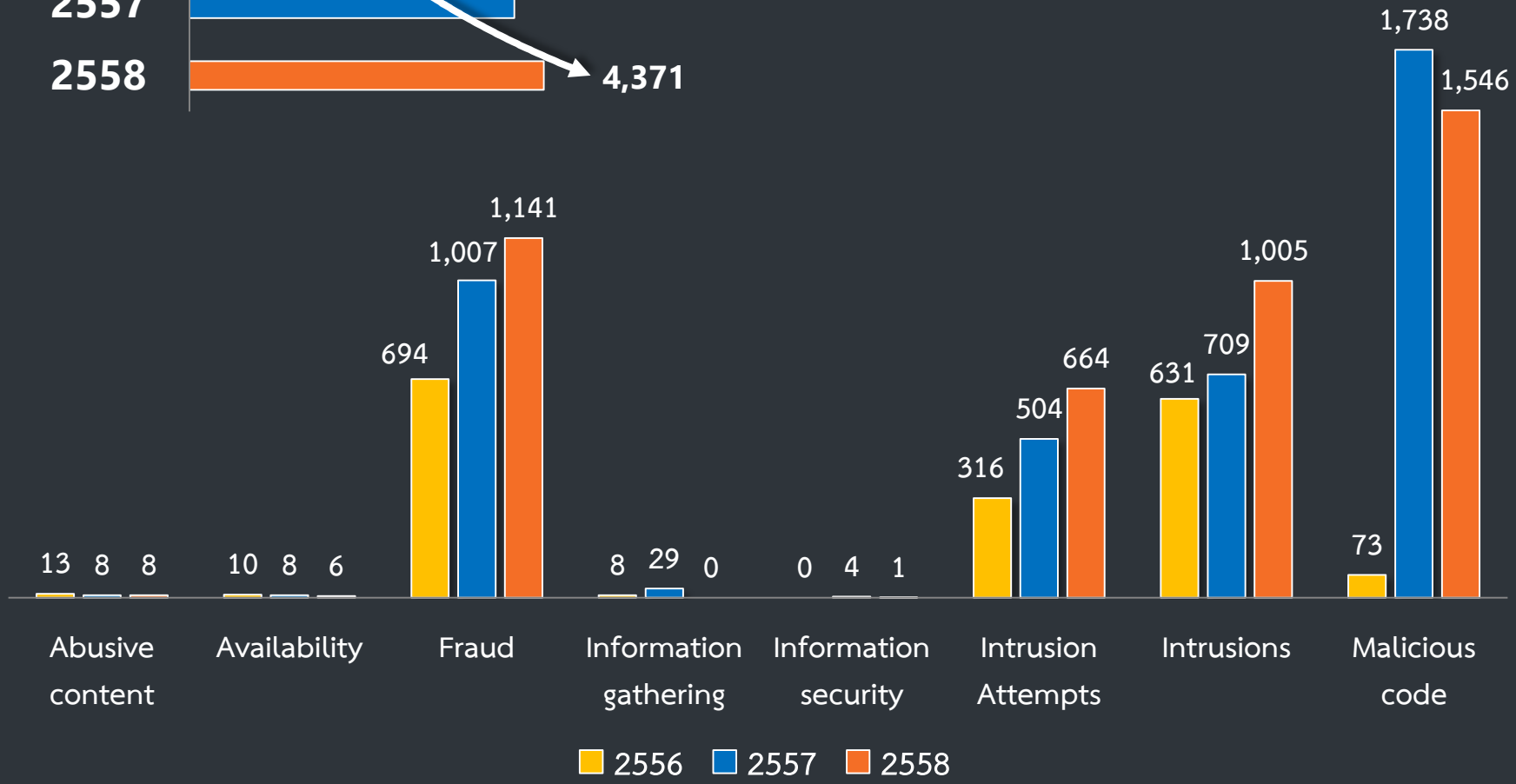
Report by Incident Type

- Malicious code 1,546 (35.3%)
- Fraud (Phishing) 1,141 (26.1%)
- Intrusion 1,005 (22.9%)

ThaiCERT Statistics

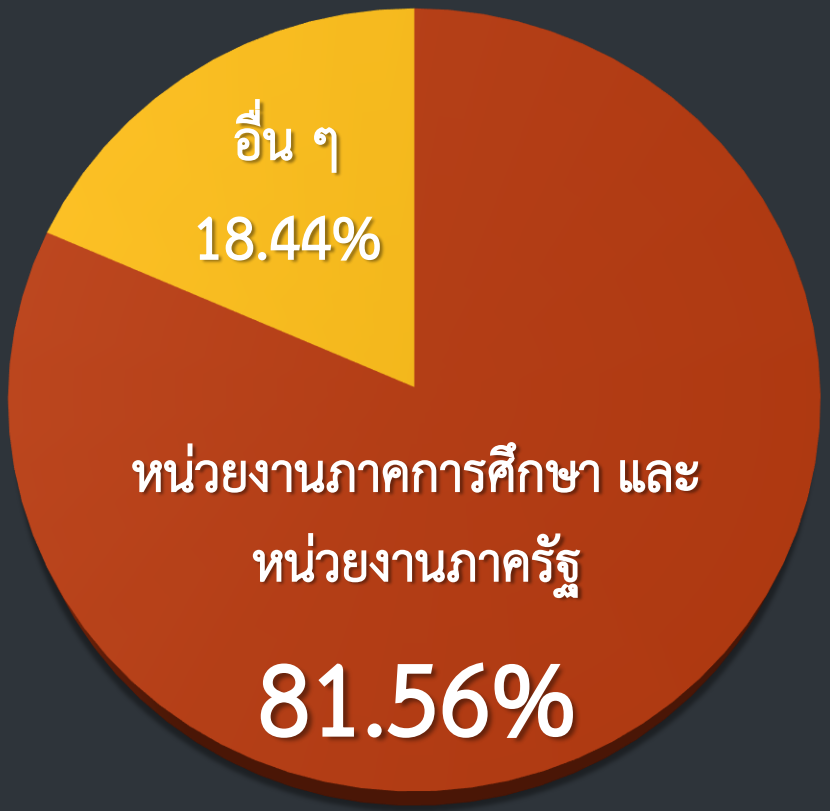
รายงานเปรียบเทียบสถิติภัยคุกคามที่ไทยเซิร์ตได้รับแจ้ง
ในปี 2556 2557 และ 2558





ThaiCERT Statistics

รายงานเปรียบเทียบสถิติภัยคุกคามประเภทการโจมตีเว็บไซต์ (Web Attack)
ของหน่วยงานในประเทศไทยที่ ThaiCERT ได้รับรายงาน

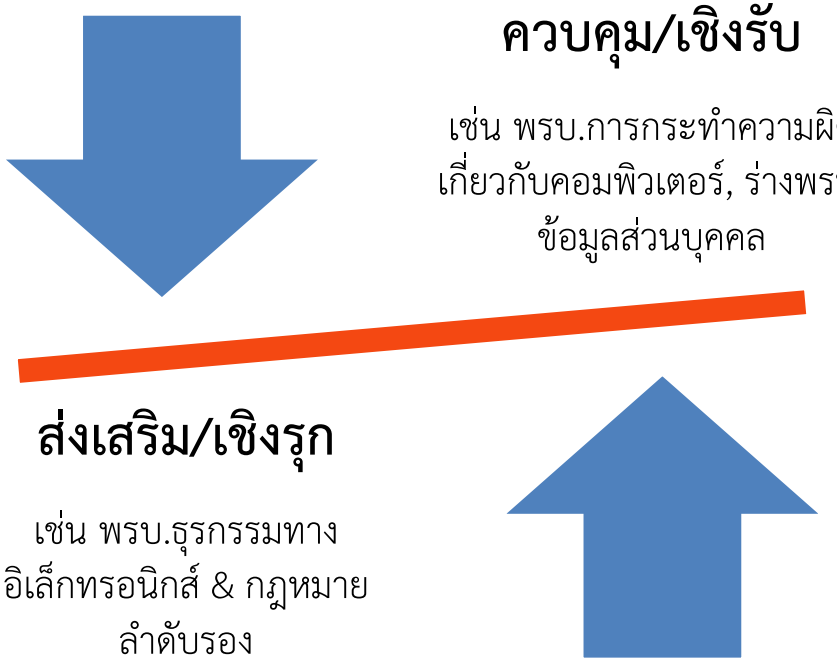


*Web Attack = Malware URL, Phishing, and Web Defacement

กฎหมายเทคโนโลยีสารสนเทศ

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

บทบาทของกฎหมาย IT



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.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

กฎหมาย IT ฉบับแรกของไทย

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551

พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ..) พ.ศ. ....

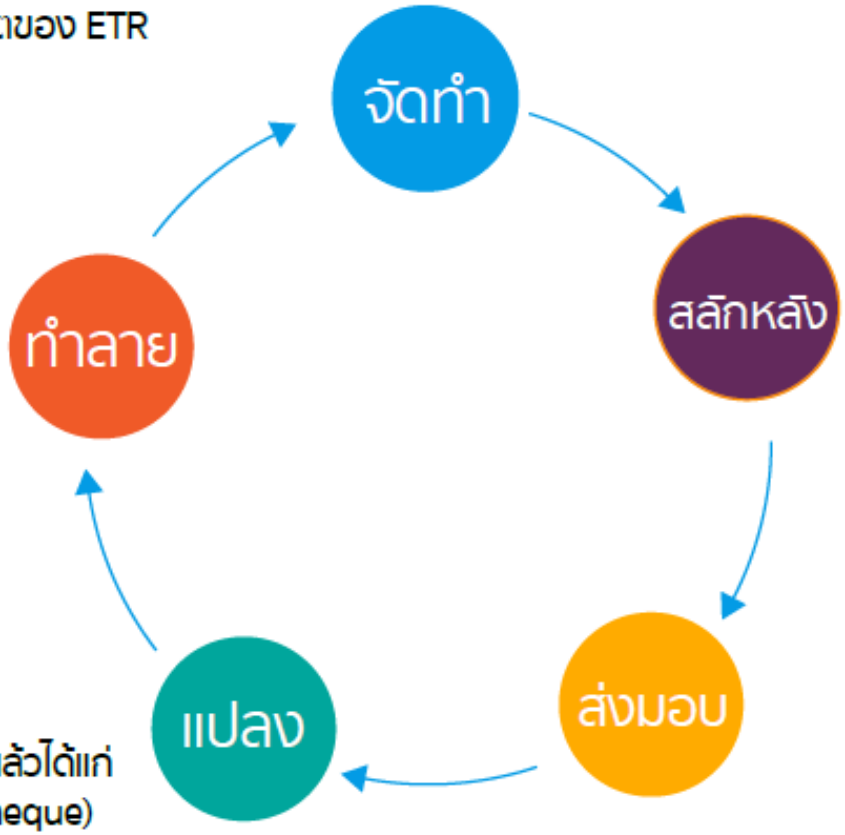
การพัฒนาในอนาคต

Electronic Transferable Records

Online Dispute Resolution

e-Transferable Record (ETR)
เอกสารที่เปลี่ยนมือได้ทางอิเล็กทรอนิกส์

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



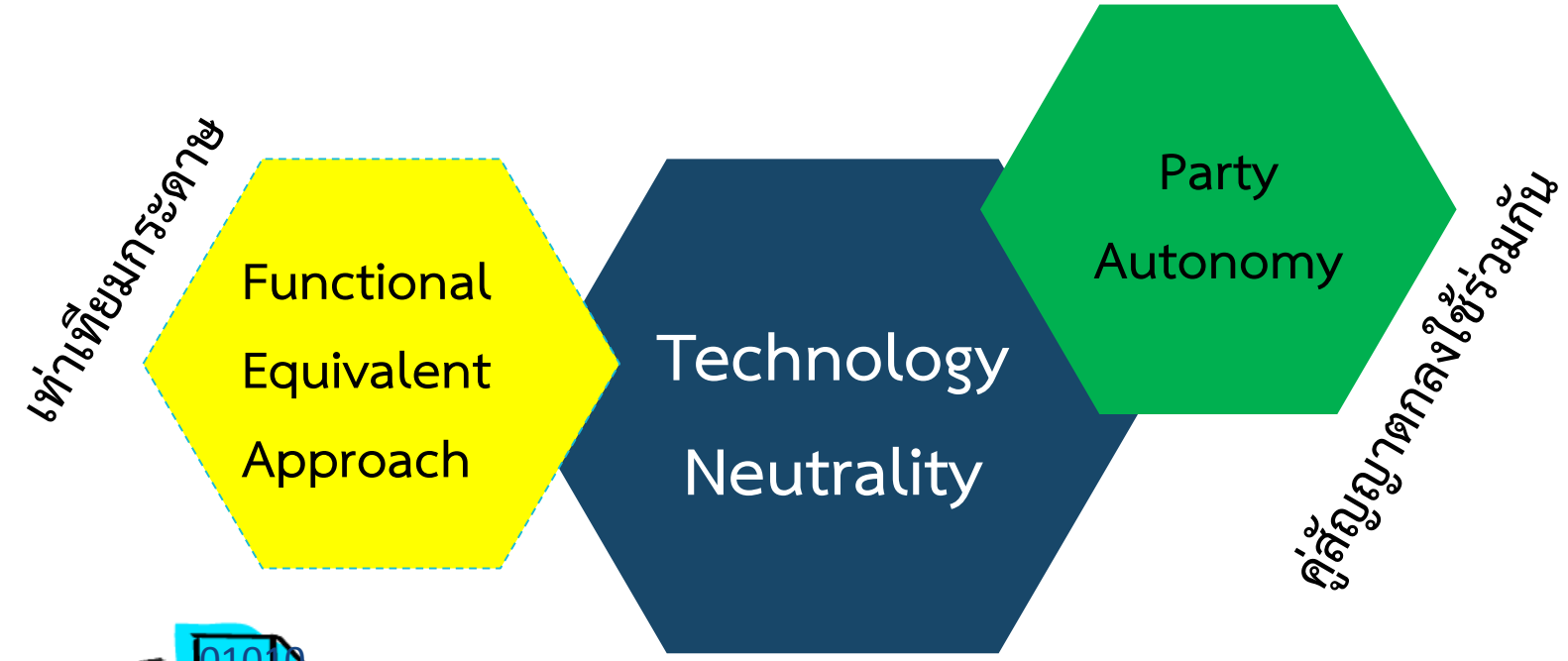
- ปัจจุบัน ประเทศที่มีกฎหมายรองรับเรื่อง ETR แล้วได้แก่ เกาหลีใต้ (e-Promissory Note) ฮ่องกง (e-Cheque)

[Online Dispute Resolution]

ONLINE DISPUTE RESOLUTION FOR CROSS-BORDER ELECTRONIC COMMERCE TRANSACTION:

3 STAGES :

หลักการพื้นฐานธุรกรรมทางอิเล็กทรอนิกส์



ใช้บังคับเพื่อเสริมกฎหมายอื่น

(เสริมให้ทำในรูปแบบอิเล็กทรอนิกส์ได้)

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ฯ → **เสริม** → **ประมวลกฎหมายแพ่งและพาณิชย์ (มาตรา 861 – 897)**

รองรับให้ธุรกรรมกระดาษตามที่กำหนดในกฎหมายต่าง ๆ ทำในรูปแบบข้อมูลอิเล็กทรอนิกส์ได้

ตัวอย่าง

มาตรา ๘๖๗ อันสัญญาประกันภัยนั้น ถ้ามิได้มีหลักฐานเป็นหนังสืออย่างใดอย่างหนึ่งลงลายมือชื่อฝ่ายที่ต้องรับผิดหรือลายมือชื่อตัวแทนของฝ่ายนั้นเป็นสำคัญ ท่านว่าจะฟ้องร้องให้บังคับคดีหาได้ไม่

ให้ส่งมอบกรมธรรม์ประกันภัยอันมีเนื้อความต้องตามสัญญานั้นแก่ผู้เอาประกันภัยฉบับหนึ่ง

กรมธรรม์ประกันภัย ต้องลงลายมือชื่อของผู้รับประกันภัยและมีรายการดังต่อไปนี้

หมายเหตุ กฎหมายธุรกรรมทางอิเล็กทรอนิกส์ไม่ใช้กับ (1) ธุรกรรมเกี่ยวกับครอบครัว

(2) ธุรกรรมเกี่ยวกับมรดก

เสริมกฎหมายอื่นๆ ให้ทำเป็นอิเล็กทรอนิกส์ได้

แต่ไม่มีผลกระทบกระเทือนถึงกฎหมายหรือกฎใดที่กำหนดขึ้นเพื่อคุ้มครองผู้บริโภค

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

ตัวอย่าง

กฎหมายคุ้มครองผู้บริโภค

- พระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2552 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 3) พ.ศ. 2556
- พระราชบัญญัติอาหาร พ.ศ. 2522
- พระราชบัญญัติยา พ.ศ. 2510 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 5)พ.ศ.2530

ทำไมต้องรู้ว่าอะไรคือสิ่งที่กฎหมายกำหนด และอะไรเป็นขั้นตอนของเราเอง

Law

ต้องปฏิบัติตาม

กฎหมายกำหนดแบบ ขั้นตอน เงื่อนไข อย่างไรบ้าง

(หากกฎหมายข้อไหนจะเป็นอุปสรรค/ไม่จำเป็นสำหรับระบบอิเล็กทรอนิกส์
ต้องเสนอแก้ไขกฎหมาย)

Business Process

ปรับเปลี่ยนให้เหมาะสมกับระบบอิเล็กทรอนิกส์

ขั้นตอนภายในของเรากำหนด Business Process ไว้อย่างไร

(หากขั้นตอนไหนเป็นอุปสรรค/ไม่จำเป็นสำหรับระบบอิเล็กทรอนิกส์
เสนอผู้บริหารเพื่อปรับเปลี่ยนแก้ไข)

โครงกฎหมาย

“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

สามารถตกลงร่วมกันในกลุ่มธุรกิจเพื่อให้เป็นมาตรฐานเดียวกันได้

ELECTRONIC DOCUMENT ม. 8

1. เข้าถึงได้

2. นำกลับมาใช้ได้

3. ความหมายไม่เปลี่ยนแปลง

e-SIGNATURE ม. 9

1. ระบุตัวผู้เป็นเจ้าของลายมือชื่อได้

2. แสดงได้ว่าเจ้าของลายมือชื่อยอมรับข้อความนั้น

3. ใช้วิธีการที่น่าเชื่อถือ
   - ความมั่นคงและรัดกุมของวิธีการที่ใช้
   - ลักษณะ ประเภท หรือขนาดของธุรกรรมที่ทำฯลฯ
   - ความรัดกุมของระบบติดต่อสื่อสาร

E-SIGNATURE

ลายมือชื่อ
ที่เชื่อถือได้

ม. 9

1. ระบุตัวผู้เป็นเจ้าของ
ลายมือชื่อได้

2. แสดงได้ว่าเจ้าของ
ลายมือชื่อ
ยอมรับข้อความนั้น

3. ใช้วิธีการที่น่าเชื่อถือ

ม. 26

1. ข้อมูลที่ใช้สร้างลายมือชื่อ
เชื่อมโยงไปยังเจ้าของได้

2. ข้อมูลที่ใช้สร้างลายมือชื่ออยู่ภายใต้
การควบคุมของเจ้าของ เมื่อสร้าง

3. สามารถตรวจพบการ
เปลี่ยนแปลงของลายมือชื่อ /
ข้อความ นับแต่สร้างได้

ม. 10 ความเป็นต้นฉบับของข้อมูลอิเล็กทรอนิกส์

(๑) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์

(๒) สามารถแสดงข้อความนั้นในภายหลังได้

ทำไมต้องต้นฉบับ ?

ความถูกต้องดูจากอะไร ?

ความครบถ้วนและไม่มีการเปลี่ยนแปลงใดของข้อความ

เว้นแต่การรับรองหรือบันทึกเพิ่มเติม หรือการเปลี่ยนแปลงใดๆ ที่อาจจะเกิดขึ้นได้ตามปกติในการติดต่อสื่อสาร การเก็บรักษา หรือการแสดงข้อความซึ่งไม่มีผลต่อความถูกต้องของข้อความนั้น

ม. 12 การเก็บรักษาข้อมูลอิเล็กทรอนิกส์

(๑) ข้อมูลอิเล็กทรอนิกส์นั้นสามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง

(๒) ได้เก็บรักษาข้อมูลอิเล็กทรอนิกส์นั้นให้อยู่ในรูปแบบที่เป็นอยู่ในขณะที่สร้าง ส่ง หรือได้รับข้อมูลอิเล็กทรอนิกส์นั้น หรืออยู่ในรูปแบบที่สามารถแสดงข้อความที่สร้าง ส่ง หรือได้รับให้ปรากฏอย่างถูกต้องได้ และ

(๓) ได้เก็บรักษาข้อความส่วนที่ระบุถึงแหล่งกำเนิด ต้นทาง และปลายทางของข้อมูลอิเล็กทรอนิกส์ ตลอดจนวันและเวลาที่ส่งหรือได้รับข้อความดังกล่าว ถ้ามี

TRANSITION PERIOD

Paper ⇄ e-Doc

ม. ๑๐ วรรค ๔ — สิ่งพิมพ์ออก (printout)

อิเล็กทรอนิกส์ ⟹ กระดาษ

ม. ๑๒ — การแปลงเอกสารกระดาษเป็นเอกสารอิเล็กทรอนิกส์

กระดาษ ⟹ อิเล็กทรอนิกส์

การรับรองสิ่งพิมพ์ออก (PRINTOUT)
มาตรา 10 วรรค 4

รับรองให้printout มีผลเป็นต้นฉบับ เป็นพยานหลักฐานใช้ได้ตามกฎหมาย

ข้อความในสิ่งพิมพ์ออกถูกต้องครบถ้วน

มีการรับรองระบบการพิมพ์ออก
โดยหน่วยงานที่กำหนด

การรับรองระบบการพิมพ์ออก ทำเมื่อมีการพิมพ์ออกไปยังระบบอื่น ที่ไม่ใช่ของผู้จัดทำ

แต่ หากเป็นการพิมพ์ออกของหน่วยงานของรัฐที่มีอำนาจจัดเก็บข้อมูล/
หน่วยงานของรัฐที่เป็น regulator / หน่วยงานภายใต้การกำกับของ regulator
"ก็ไม่ต้องรับรองระบบการพิมพ์ออก"

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง การรับรองสิ่งพิมพ์ออก พ.ศ. ๒๕๕๕

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หน่วยงานรับรองสิ่งพิมพ์ออก พ.ศ. ๒๕๕๕

การแปลงเอกสาร (มาตรา 12/1)

การแปลงเอกสารทั่วไป

การแปลงเอกสารสำหรับระบบ ICAS

รับรองให้ข้อมูลอิเล็กทรอนิกส์ ที่ได้จากการแปลงเอกสารมีผลเป็นต้นฉบับ / ใช้เป็นพยานหลักฐาน/ใช้ได้ตามกฎหมาย

องค์ประกอบของการแปลง

- ความหมาย/รูปแบบ "เหมือน" กับเอกสารหรือข้อความเดิม
- วิธีการที่เชื่อถือได้ในการระบุตัวตนผู้จัดทำหรือแปลง
- ต้องมีเทคโนโลยีและมาตรการป้องกันมิให้มีการเปลี่ยนแปลงหรือแก้ไข

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องหลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. 2553

ม. ๑๑ ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในศาล

กฎหมายห้ามมิให้ปฏิเสธการรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์

(Admissibility of evidence in court)

แต่ การที่ศาลจะเชื่อถือในพยานหลักฐานทางอิเล็กทรอนิกส์หรือไม่ ขึ้นอยู่กับ

- **ความน่าเชื่อถือของพยานหลักฐาน**
- **การชั่งน้ำหนักพยานหลักฐานของศาลเอง**

e-EVIDENCE

ความน่าเชื่อถือของพยานหลักฐานดูจาก

- ลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์
- ลักษณะหรือวิธีการเก็บรักษาความครบถ้วนและไม่มีการเปลี่ยนแปลง
- ลักษณะ วิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล
- รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง

มาตรา 25
วิธีการแบบปลอดภัย
(การปฏิบัติตามมาตรา 25 จะได้ประโยชน์จากข้อสันนิษฐานทางกฎหมาย)

การยกระดับความมั่นคงปลอดภัย และความน่าเชื่อถือของการทำธุรกรรมทางอิเล็กทรอนิกส์สำหรับธุรกิจประกันภัย

มาตรา 25 แห่ง พ.ร.บ. ธุรกรรมฯ

+

พ.ร.ฎ.ว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553

เป็นการรักษาความมั่นคงปลอดภัย ให้มีการยอมรับและเชื่อมั่นในข้อมูลอิเล็กทรอนิกส์เพิ่มมากยิ่งขึ้น

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย ปฏิบัติได้ดังนี้

- การสร้างความมั่นคงปลอดภัยด้านการบริหารจัดการและระบบสารสนเทศ
- การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์หรือควบคุมการเข้าถึงข้อมูลอิเล็กทรอนิกส์
- การบริหารจัดการด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์และไม่อาจคาดคิด
- การบริหารจัดการด้านบริการให้มีความต่อเนื่อง

เป็นต้น

ผล

เมื่อปฏิบัติตามวิธีการแบบปลอดภัยตามระดับของตนแล้ว จะได้ประโยชน์จาก**ข้อสันนิษฐานของกฎหมาย** ว่าได้ใช้วิธีการที่น่าเชื่อถือ

การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบมั่นคงปลอดภัย

(ประกาศ คธอ. เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555)

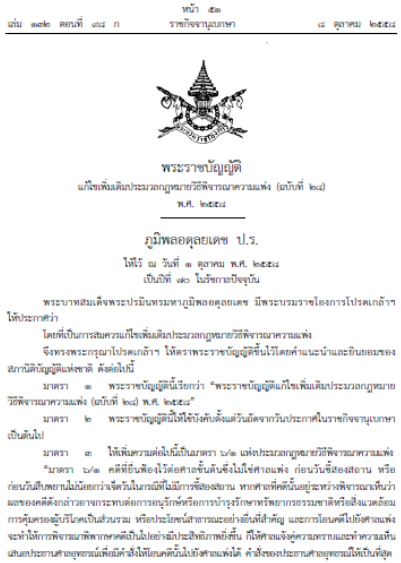
การประเมินระดับผลกระทบที่เกิดขึ้นใน 1 วัน	Security Basic ผลกระทบระดับต่ำ	Security Medium ผลกระทบระดับกลาง	Security High Level ผลกระทบระดับสูง
(1) ผลกระทบด้านมูลค่าความเสียหายทางการเงิน	≤ 1 ล้านบาท	≧ 1 ล้านบาท ≤ 100 ล้านบาท	≧ 100 ล้านบาท
(2) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับอันตรายต่อชีวิต ร่างการหรือนามัย	ไม่มีผู้ใช้บริการได้รับผลกระทบต่อชีวิต ร่างกาย หรืออนามัย	ผู้ใช้บริการได้รับผลกระทบต่อร่างกาย หรืออนามัย ≧ 1 คน ≤ 1,000 คน	ผู้ใช้บริการได้รับผลกระทบต่อร่างกายหรืออนามัย ≧ 1,000 คน หรือต่อชีวิตตั้งแต่ 1 คน
(3) ผลกระทบต่อจำนวนผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายอื่นใดนอกจาก (2)	ผู้ใช้บริการได้รับผลกระทบ ≤ 10,000 คน	ผู้ใช้บริการได้รับผลกระทบ ≧ 10,000 คน แต่ ≤ 100,000 คน	ผู้ใช้บริการได้รับผลกระทบ ≧ 100,000 คน
(4) ผลกระทบด้านความมั่นคงของรัฐ	**ไม่มี**ผลกระทบต่อความมั่นคงของรัฐ	-	**มี**ผลกระทบต่อความมั่นคงของรัฐ
		หากมีผลกระทบระดับกลางอย่างน้อย 2 ด้านขึ้นไปให้ใช้วิธีการแบบปลอดภัยในระดับกลางขึ้นไป	หากมีผลกระทบระดับสูงเพียง 1 ด้านต้องใช้วิธีการแบบมั่นคงปลอดภัยในระดับเคร่งครัด

ตัวอย่างการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐาน

ฎีกาที่ 8089/2556

- การเบิกถอนเงินสดจากบัญชีสินเชื่อเงินสด ผ่านตู้ ATM เป็นธุรกรรมทางอิเล็กทรอนิกส์ ซึ่งรับฟังได้ตามมาตรา 7
- การนำบัตรกดเงินสดไปถอนเงินและใส่รหัสส่วนตัว เสมือนการลงลายมือชื่อตนเอง ซึ่งถือเป็นการลงลายมือชื่ออิเล็กทรอนิกส์ตามมาตรา 9
- เมื่อจำเลยนำบัตรกดเงินสดไปถอนเงิน ใส่รหัสเพื่อทำรายการถอนเงิน และกดยินยันทำรายการ พร้อมรับเงินสดและสลิป การกระทำดังกล่าวจึงถือเป็นหลักฐานการกู้ยืมเงิน ตามมาตรา 8 วรรคหนึ่ง

[ทิศทางการพัฒนา e-Court]



พระราชบัญญัติ
แก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง (ฉบับที่ ๒๘)
พ.ศ. ๒๕๕๘

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๑ ตุลาคม พ.ศ. ๒๕๕๘
เป็นปีที่ ๗๐ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

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

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๖/๑ แห่งประมวลกฎหมายวิธีพิจารณาความแพ่ง

"มาตรา ๖/๑ คดีที่ยื่นฟ้องไว้ต่อศาลชั้นต้นซึ่งไม่ใช่ศาลแพ่ง ก่อนวันชี้สองสถาน หรือก่อนวันสืบพยานไม่น้อยกว่าเจ็ดวันในกรณีที่ไม่มีการชี้สองสถาน หากศาลที่คดีนั้นอยู่ระหว่างพิจารณาเห็นว่าผลของคดีดังกล่าวอาจกระทบต่อการอนุรักษ์หรือการบำรุงรักษาหรือขยายทรัพยากรธรรมชาติหรือสิ่งแวดล้อม การคุ้มครองผู้บริโภคเป็นส่วนรวม หรือประโยชน์สาธารณะอย่างอื่นที่สำคัญ และการโอนคดีไปยังศาลแพ่งจะทำให้การพิจารณาพิพากษาคดีเป็นไปอย่างมีประสิทธิภาพยิ่งขึ้น ก็ให้ศาลแจ้งคู่ความทราบและทำความเห็นเสนอประธานศาลอุทธรณ์เพื่อมีคำสั่งให้โอนคดีนั้นไปยังศาลแพ่งได้ คำสั่งของประธานศาลอุทธรณ์ให้เป็นที่สุด

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

ประกาศราชกิจจานุเบกษาเมื่อ 8 ตุลาคม 2558

- รองรับการจัดทำสารบบความ สำนวนความในรูปแบบข้อมูลอิเล็กทรอนิกส์ รวมถึง Print out ของข้อมูลดังกล่าว
- รองรับการยื่นคำคู่ความและเอกสารในรูปแบบข้อมูลอิเล็กทรอนิกส์ เช่น ผ่านอีเมล

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

อาศัยอำนาจ ม. 35 พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์

"หน่วยงานของรัฐ" (มาตรา 4)

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

กำหนดหลักเกณฑ์ 3 เรื่อง ได้แก่

การจัดให้มีระบบเอกสารที่ทำในรูปข้อมูลอิเล็กทรอนิกส์ (ม. 3 และ ม. 4)

- รูปแบบที่เหมาะสม & แสดงหรืออ้างอิงได้ในภายหลัง & ข้อความครบถ้วน
- กำหนดระยะเวลาเริ่มต้นหรือสิ้นสุดและอาจกำหนดระยะเวลาดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

จัดให้มีแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Security Policy) (ม. 5)

ประกาศ คธอ. เรื่อง แนวนโยบาย/แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2553

จัดให้มีแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล (privacy policy) (ม. 6)

ประกาศ คธอ. เรื่อง แนวนโยบาย/แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

ต้องได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

หน่วยงานของรัฐนำไปปฏิบัติ

ตรวจสอบการนำไปปฏิบัติ

Security

ประกาศ คธอ. เรื่อง แนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และฉบับที่ 2 พ.ศ. 2556

นโยบาย (Policy)

1. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
2. การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน
3. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อปฏิบัติ (Practice)

1. การเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control)
2. การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control)
3. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)
4. หน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)
5. ควบคุมการเข้าถึงเครือข่าย (network access control)
6. การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)
7. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control)
8. จัดทำระบบสำรอง
9. ให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
10. กำหนดหน้าที่ความรับผิดชอบที่ชัดเจน หากเกิดกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใด

Data Protection

ประกาศ คธอ. เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553

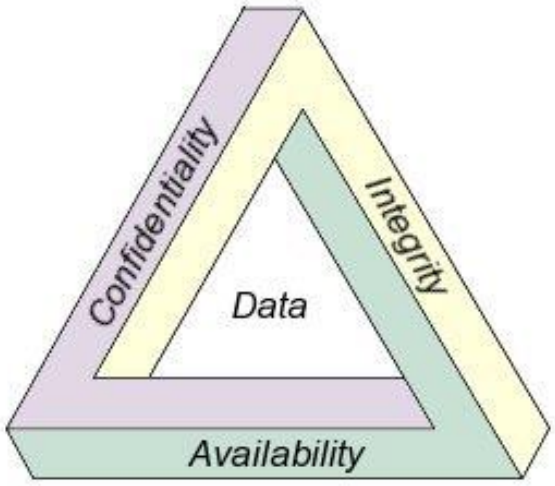
นโยบายและข้อปฏิบัติต้องสอดคล้องกันและต้องคำนึงถึงหลักเกณฑ์ 8 ประการ ดังนี้

สอดคล้องกับ OECD

1. การเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด (Collection Limitation Principle)
2. คุณภาพของข้อมูลส่วนบุคคล (Data Quality Principle)
3. การระบุวัตถุประสงค์ในการเก็บรวบรวม (Purpose Specification Principle)
4. ข้อจำกัดในการนำข้อมูลส่วนบุคคลไปใช้ (Use Limitation Principle)
5. การรักษาความมั่นคงปลอดภัย (Security Safeguards Principle)
6. การเปิดเผยเกี่ยวกับการดำเนินการ แนวปฏิบัติ และนโยบายที่เกี่ยวกับข้อมูลส่วนบุคคล (Openness Principle)
7. การมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)
8. ความรับผิดชอบของบุคคลซึ่งทำหน้าที่ควบคุมข้อมูล (Accountability Principle)

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

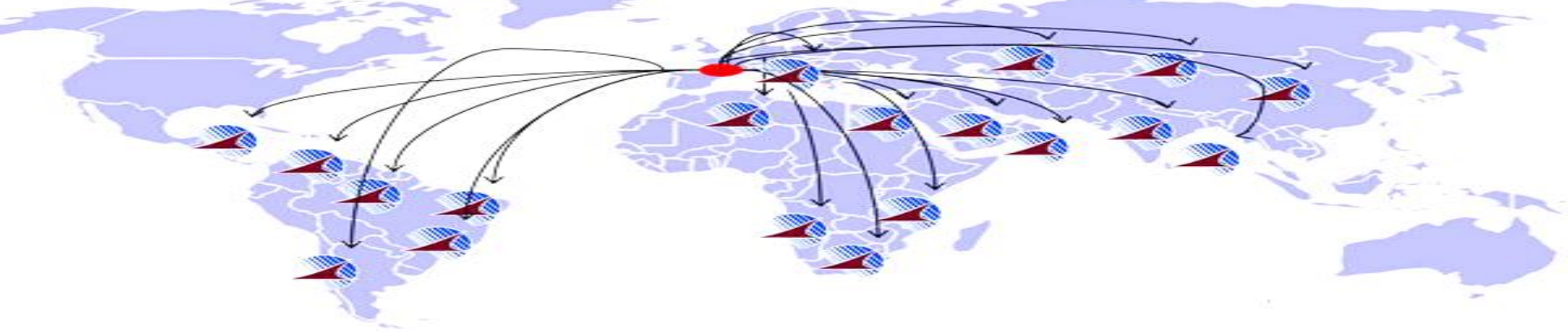
กำหนดมาตรการในการป้องกัน
และปราบปรามการกระทำ
ความผิดเกี่ยวกับคอมพิวเตอร์



รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (**Authenticity**) ความรับผิด (**Accountability**) การห้ามปฏิเสธความรับผิด (**Non-repudiation**) และความน่าเชื่อถือ (**Reliability**)

ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)

C.I.A. = หลักการพื้นฐานของ Information Security และ Cybersecurity



รูปแบบและฐานความผิดทางอาชญากรรมทางคอมพิวเตอร์

ลักษณะของอาชญากรรมทางคอมพิวเตอร์

- ผู้กระทำความผิดอยู่ตรงไหนก็ได้ในโลก
- ความเสียหายกระทบถึงคนจำนวนมาก & รวดเร็ว
- ใช้เทคโนโลยีที่ซับซ้อนในการกระทำความผิด
- ยากต่อการตรวจพบร่องรอยการกระทำผิด
- ยากต่อการจับกุมและนำผู้กระทำผิดมาลงโทษ
- สามารถริเริ่มการกระทำความผิดครั้งใหม่ได้โดยรวดเร็ว

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

บททั่วไป

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

ม.12 บทหนัก

กระทำความผิดนอกราชอาณาจักร ต้องรับโทษภายในราชอาณาจักร์ (ม.17)

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

หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์

กระทำต่อคอมพิวเตอร์

- **ม.5** การเข้าถึงระบบคอมฯ
- **ม.6** การล่วงรู้มาตรการการป้องกันการเข้าถึง
- **ม.7** การเข้าถึงข้อมูลคอมฯ
- **ม.8** การดักรับข้อมูลคอมฯ
- **ม.9** การรบกวนข้อมูลคอมฯ
- **ม.10** การรบกวนระบบคอมฯ
- **ม.13** การจำหน่าย/ เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด

ใช้คอมพิวเตอร์กระทำความผิด

- **ม.11** Spam mail
- **ม.14** การปลอมแปลงข้อมูลคอมพิวเตอร์/เผยแพร่เนื้อหาอันไม่เหมาะสม
- **ม.15** ความรับผิดของผู้ให้บริการ
- **ม.16** การเผยแพร่ภาพจากการตัดต่อ/ดัดแปลง

หมวด 2 พนักงานเจ้าหน้าที่

พนักงานเจ้าหน้าที่

อำนาจหน้าที่ (ม.18) : (1) มีหนังสือ/เรียกเพื่อให้ถ้อยคำ/เอกสาร (2) เรียกข้อมูลจราจร (3) สั่งให้ส่งมอบข้อมูลที่อยู่ในครอบครอง (4) ทำสำเนาข้อมูล (5) สั่งให้ส่งมอบข้อมูล/อุปกรณ์ (6) ตรวจสอบ/เข้าถึง (7) ถอดรหัสลับ (8) ยึด/อายัดระบบ

ข้อจำกัด/การตรวจสอบการใช้อำนาจ (ม.19) : ยื่นคำร้องต่อศาลในการใช้อำนาจตาม ม.18 (4)-(8), ส่งสำเนาบันทึกรายละเอียดให้แก่ศาลภายใน 48 ชม., ยึด/อายัดห้ามเกิน 30 วัน ขอขยายได้อีก 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 ระวางโทษปรับ

กฎหมายลำดับรองภายใต้พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ม.๑๙ แบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์	กฎกระทรวงกำหนดแบบหนังสือแสดงการยึดหรืออายัดระบบคอมพิวเตอร์ พ.ศ ๒๕๕๑
ม.๒๖ หน้าที่ของผู้ให้บริการในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์	ประกาศ ทก. เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐
ม.๒๘ คุณสมบัติของพนักงานเจ้าหน้าที่	ประกาศ ทก. เรื่อง หลักเกณฑ์เกี่ยวกับการกำหนดคุณสมบัติของพนักงานเจ้าหน้าที่ฯ
ม.๒๙ อำนาจพนักงานเจ้าหน้าที่	ระเบียบว่าด้วยการจับ ควบคุม ค้น การทำสำนวนสอบสวนและดำเนินคดีกับผู้กระทำความผิดตาม พ.ร.บ.คอมฯ พ.ศ. ๒๕๕๐
ม.๓๐ บัตรประจำตัวของพนักงานเจ้าหน้าที่	ประกาศ ทก. เรื่อง กำหนดแบบบัตรประจำตัวพนักงานเจ้าหน้าที่ฯ

หน้าที่ของผู้ให้บริการ ภายใต้กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ม.26 หน้าที่ของผู้ให้บริการ cloud ในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

<u>หากไม่ปฏิบัติตาม</u> ผู้ให้บริการถูกปรับไม่เกิน 500,000 บาท

- เก็บรักษา**ข้อมูลจราจรทางคอมพิวเตอร์**เท่าที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้บริการ**ไม่น้อยกว่า 90 วัน** นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ (รัฐมนตรีจะเป็นผู้ประกาศในราชกิจจานุเบกษาว่ากรณีดังกล่าวจะใช้บังคับกับผู้ให้บริการประเภทใด)
- **ในกรณีจำเป็น** พนักงานเจ้าหน้าที่สามารถสั่งผู้ให้บริการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์**เกิน 90 วันได้ แต่ต้องไม่เกิน 1 ปี**

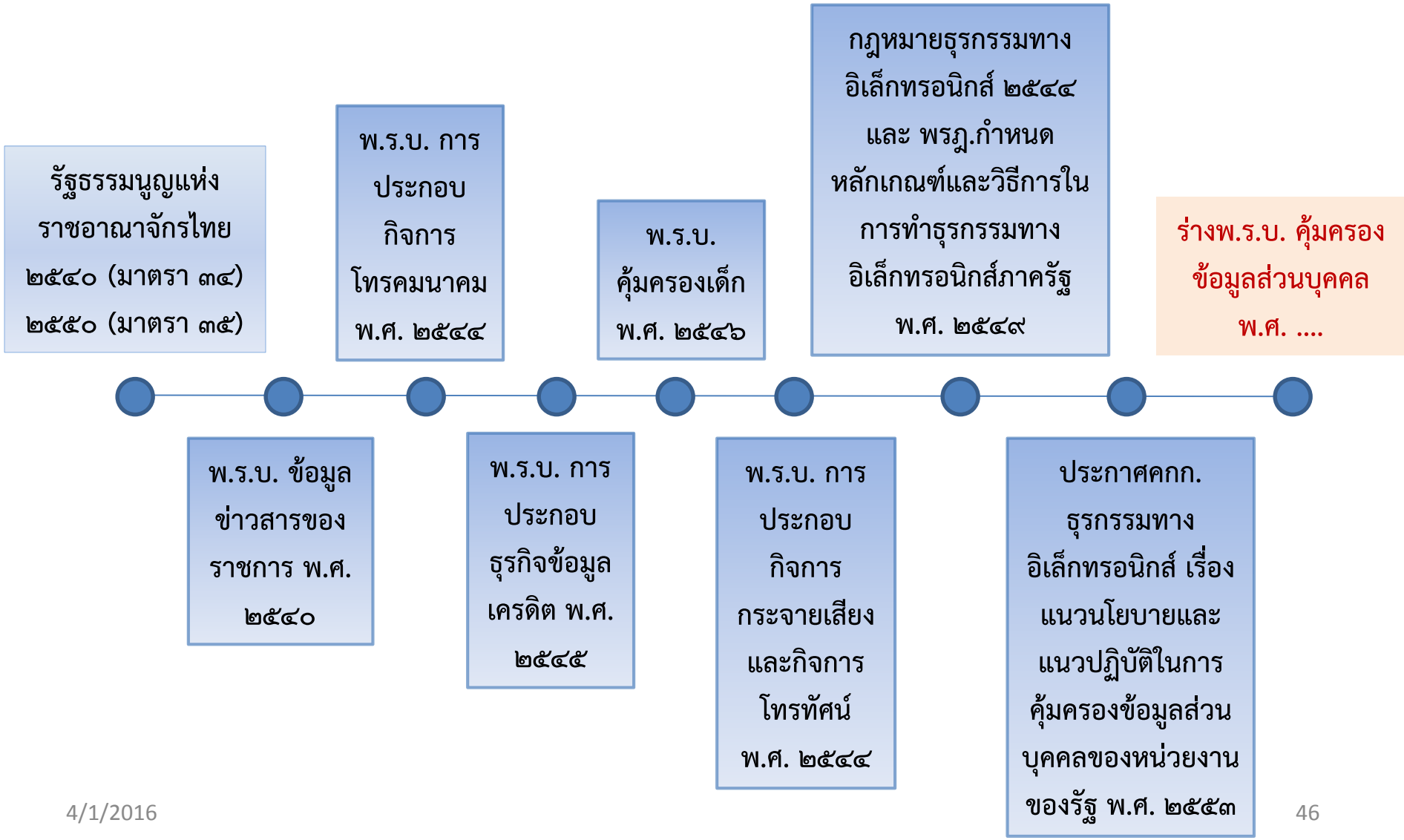
หลักเกณฑ์การเก็บข้อมูลจารจรคอมพิวเตอร์

ประกาศ ทก. เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550

- ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการมีหน้าที่ต้องเก็บรักษา
- การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้มั่นคงปลอดภัย

* ข้อมูลจราจรทางคอมพิวเตอร์ คือ ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรือ อื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

พัฒนาการด้านกฎหมายกับการคุ้มครองข้อมูลส่วนบุคคล



International Law: OECD APEC EU

OECD Guideline

- OECD Guidelines on the protection of privacy and transborder flows of personal data

APEC Framework

- APEC Privacy Framework

European Union

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

U.S. EU SAFEHARBOR

European Union

United States of America

Under Safe Harbor, a U.S. company can self-certify annually to the Department of Commerce that is has complied with the seven basic principles and related requirements that have been deemed to meet the data privacy adequacy standard of the EU

Maximillian Case: the ECJ rejecting Safe Harbour

Press and Information

Court of Justice of the European Union

Luxembourg, 6 October 2015

Maximillian Schrems v Data Protection Commissioner

The Court of Justice declares that

the Commission's US Safe Harbour Decision is invalid.

The EU Countries can choose to suspend the transfer of data to the US

http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

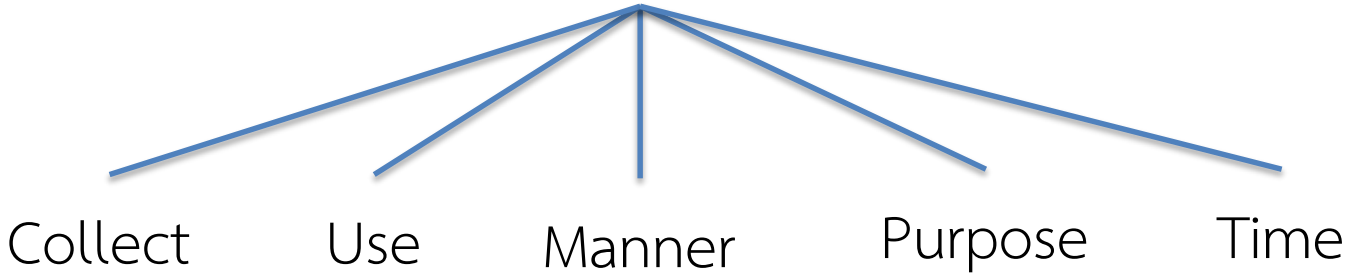
สภาพปัญหา	**การละเมิดข้อมูลส่วนบุคคลรุนแรงมากขึ้น IoT, Cloud, Big Data**
ความจำเป็นในการตรากม.	**- กำหนดมาตรการคุ้มครองที่เพียงพอและเหมาะสม** **- ข้อกำหนดในเวทีระดับประเทศมีอิทธิพลต่อไทย** OECD / EU Directive (Supra-national) UN / APEC / Privacy Commissioner **- กฎหมายในประเทศมีอยู่บ้าง แต่ไม่ครบ และบางส่วนแย้งกันเอง (ขาดกฎหมายกลาง)** ขาดมาตรการการคุ้มครองที่เหมาะสม

ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

Concept

CONTROL

Your Personal Data, Your Choice



ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

บุคคลที่เกี่ยวข้องตามกฎหมาย

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้ ***สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม***...

ตัวอย่าง ชื่อ นามสกุล เพศ รูปถ่าย ที่อยู่ อีเมล เบอร์โทรศัพท์ ข้อมูลสุขภาพ ข้อมูลทางการเงิน รหัสบัตรเครดิต รหัสบัตรประชาชน IP Address ความชอบส่วนบุคคล (สี อาหาร เสื้อผ้า ท่องเที่ยว งานอดิเรก) ความเห็นทางการเมือง

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่ง ***มีอำนาจหน้าที่ตัดสินใจ***เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล”

ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

หน้าที่ของผู้ควบคุมของข้อมูลส่วนบุคคล

การเก็บรวบรวม ใช้ เปิดเผย

✓ **ขอความยินยอม** เมื่อเก็บรวบรวม ใช้และการเปิดเผย

วัตถุประสงค์

✓ **แจ้งวัตถุประสงค์**ให้เจ้าของข้อมูลทราบ ก่อนหรือขณะเก็บข้อมูล

✓ **ใช้ตามวัตถุประสงค์**ที่ได้มีการแจ้ง

ความปลอดภัย

✓ จัดให้มีมาตรการรักษา**ความมั่นคงปลอดภัย**

✓ ทำให้**ข้อมูลถูกต้อง ทันสมัย สมบูรณ์**

✓ **ทำลาย**ข้อมูลเมื่อพ้นกำหนดเวลา

การใช้ outsource

✓ หากใช้ Outsource ต้องจัด

มาตรการป้องกันที่เพียงพอ

แจ้งเหตุละเมิด

✓ **แจ้งเหตุละเมิด**ข้อมูลส่วนบุคคล

พร้อมจัดให้มีมาตรการเยียวยา

จัดทำรายการเพื่อตรวจสอบ

ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

หน้าที่ของผู้ควบคุมของข้อมูลส่วนบุคคล : การเก็บรวบรวม ใช้ เปิดเผย

หลักการพื้นฐานของการเก็บรวบรวม

(๑) ต้อง**เก็บเท่าที่จำเป็น** ภายใต้**วัตถุประสงค์อันชอบด้วยกฎหมาย**

(๒) ต้อง**แจ้งรายละเอียดและวัตถุประสงค์**ตามที่กฎหมายกำหนด

(๓) ห้ามมิให้เก็บรวบรวมโดยไม่**ขอความยินยอม**

(๔) ต้องเก็บข้อมูลจากเจ้าของข้อมูลส่วนบุคคล**โดยตรง**

หลักพื้นฐานการใช้ หรือ เปิดเผย

(๑) ห้ามมิให้ใช้ หรือเปิดเผยโดยไม่**ขอความยินยอม**

(๒) ต้องใช้หรือเปิดเผยข้อมูล**ภายในวัตถุประสงค์เดิมที่ได้แจ้ง**ไว้ต่อเจ้าของข้อมูลส่วนบุคคล

ข้อยกเว้น เช่น เป็นการปฏิบัติตามกฎหมาย

เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ในกระบวนการพิจารณาคดี

ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

หน้าที่ของผู้ควบคุมของข้อมูลส่วนบุคคล : ความปลอดภัย

หลักเกณฑ์มาตรการรักษาความมั่นคงปลอดภัย

“จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม”

ป้องกันมิให้ผู้อื่นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ (Outsource)

หากผู้ควบคุมข้อมูลส่วนบุคคลให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคล *“ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ”*

ป้องกันข้อมูลส่วนบุคคล จากการเข้าถึงข้อมูลโดยปราศจากอำนาจ (unauthorized access), การถูกทำลาย (destruction), การใช้ (use), การเปลี่ยนแปลง (modification), และการเปิดเผยข้อมูล (disclosure)

ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

หน้าที่ของผู้ควบคุมของข้อมูลส่วนบุคคล : แจ้งเหตุละเมิด อัพเดตข้อมูล

หลักเกณฑ์การแจ้งเหตุละเมิด

ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า เพื่อให้เจ้าของข้อมูลนั้นทราบถึงเหตุละเมิดดังกล่าว

หลักเกณฑ์การอัพเดตข้อมูล

ดำเนินการให้ข้อมูลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล

สิทธิของเจ้าของข้อมูลส่วนบุคคล

ตัวอย่างสิทธิของเจ้าของข้อมูลส่วนบุคคล

1. สิทธิขอเข้าถึงข้อมูลและสิทธิขอให้เปิดเผยถึงการได้มา

2. สิทธิขอให้ดำเนินการให้ข้อมูลนั้นถูกต้องสมบูรณ์ไม่ก่อให้เกิดความเข้าใจผิด

3. สิทธิเพิกถอนความยินยอม

4. สิทธิเรียกค่าเสียหายทางแพ่ง