แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงของระบบไอซีที ในสถาบันอุดมศึกษา

สุรางคณา วายุภาพ
รองผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
(องค์การมหาชน)

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔

แนวทางการตรากฎหมาย

- UNCITRAL Model Law on Electronic Commerce 1996 and
- UNCITRAL Model Law on Electronic Signature 2001

วัตถุประสงค์

เพื่อรองรับพัฒนาการทางเทคโนโลยีเกี่ยวกับการติดต่อสื่อสารทางอิเล็กทรอนิกส์และการทำธุรกรรมทางอิเล็กทรอนิกส์

สถานะ

มีผลบังคับใช้เมื่อวันที่ 3 เมษายน 2545

หลักการพื้นฐานสำคัญ

- **หลักความเท่าเทียมกัน (Functional Equivalent Approach)**
- **หลักความเป็นกลางทางเทคโนโลยี (Technology Neutrality)**
- **หลักเสรีภาพในการแสดงเจตนา (Party Autonomy)**

โครงสร้างของพระราชบัญญัติ

สาระสำคัญ

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

หมวดที่ 1 ธุรกรรมทางอิเล็กทรอนิกส์

- บทหลัก รับรองผลทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ และลายมือชื่ออิเล็กทรอนิกส์ (มาตรา 7)
- บทขยายความ เมื่อธุรกรรมนั้น จัดทำเป็นหนังสือ, ลายมือชื่อ, ต้นฉบับ, ใช้อ้างอิงเป็นพยานหลักฐาน, และมีกฎหมายอื่นกำหนดให้เก็บรักษาเอกสาร (มาตรา 8 ถึงมาตรา 12)

หมวดที่ 2 ลายมือชื่ออิเล็กทรอนิกส์

หมวดที่ 3 ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

หมวดที่ 4 **ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ**

หมวดที่ 5 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

หมวดที่ 6 บทกำหนดโทษ

การบังคับใช้ควบคู่ไปพร้อมกันกับกฎหมายฉบับอื่นที่ใช้บังคับ
(มิใช่กฎหมายที่เข้ามาแทนที่การบังคับใช้กฎหมายฉบับอื่นๆ)

กฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔
- พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙
- พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
- ประกาศธนาคารแห่งประเทศไทย ที่ สรข. ๓/๒๕๕๒ เรื่อง นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ในการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์

พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัย ในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

วันใช้บังคับ (มาตรา ๒)

- ประกาศใช้เมื่อวันที่ ๓ กันยายน ๒๕๕๓
- ใช้บังคับเมื่อพ้น ๑๘๐ วัน นับแต่วันประกาศในราชกิจจานุเบกษา
- คณะกรรมการฯ ต้องพิจารณาทบทวนหลักเกณฑ์เกี่ยวกับวิธีการแบบปลอดภัย อย่างน้อยทุกรอบระยะเวลา ๒ ปี ทั้งนี้ โดยพิจารณาถึงความเหมาะสมและความสอดคล้องกับเทคโนโลยีที่ได้มีการพัฒนาหรือเปลี่ยนแปลงไป

ที่มา :

มาตรา ๒๕ พรบ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

"ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดในพระราชกฤษฎีกา ให้สันนิษฐานว่าเป็น**วิธีการที่เชื่อถือได้**"

ความสำคัญของวิธีการที่เชื่อถือได้

การลงลายมือชื่อ (ม.๙)	(๑) ใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์นั้นว่าเป็นของตน และ (๒) วิธีการดังกล่าวเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์ โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี
ต้นฉบับเอกสาร (ม.๑๐)	(๑) ข้อมูลอิเล็กทรอนิกส์ได้ใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความตั้งแต่การสร้างข้อความเสร็จสมบูรณ์ และ (๒) สามารถแสดงข้อความนั้นในภายหลังได
พยานหลักฐาน (ม.๑๑)	ข้อมูลอิเล็กทรอนิกส์จะเชื่อถือได้หรือไม่เพียงใดนั้นให้พิเคราะห์ถึงความน่าเชื่อถือของลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการเก็บรักษา ความครบถ้วน และไม่มีการเปลี่ยนแปลงของข้อความลักษณะ หรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง

บทนิยาม

“วิธีการแบบปลอดภัย” หมายความว่า วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์

“ความมั่นคงปลอดภัยของระบบสารสนเทศ” (information security) หมายความว่า การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

ขอบเขตการใช้บังคับ (มาตรา ๕)

(๑) ธุรกรรมทางอิเล็กทรอนิกส์ซึ่งมีผลกระทบต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน ทั้งนี้ โดยคำนึงถึง

- ระดับความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ
- ผลกระทบต่อมูลค่าและความเสียหายที่ผู้ใช้บริการอาจได้รับ
- ผลกระทบต่อเศรษฐกิจและสังคมของประเทศ

(๒) ธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงาน หรือองค์กรที่ถือเป็น**โครงสร้างพื้นฐานสำคัญของประเทศ**

โครงสร้างพื้นฐานสำคัญของประเทศ (critical infrastructure)

หมายถึง บรรดาหน่วยงาน หรือองค์กร หรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กร ซึ่งธุรกรรมทางอิเล็กทรอนิกส์**มีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศ หรือต่อสาธารณชน**

critical infrastructure

คณะอนุกรรมการด้านความมั่นคงได้แบ่งกลุ่มหน่วยงาน CI ออกเป็น 8 กลุ่ม:

- กลุ่มไฟฟ้า พลังงาน และทรัพยากรธรรมชาติ
- กลุ่มเกษตรกรรม อาหาร น้ำ และยา
- กลุ่มการเงิน การคลัง การธนาคาร การประกันภัย และหลักทรัพย์
- กลุ่มสื่อสาร โทรคมนาคม ขนส่ง และสื่อสารมวลชน
- กลุ่มข้อมูลสารสนเทศ และระบบเทคโนโลยีสารสนเทศ
- กลุ่มความมั่นคงของประเทศ
- กลุ่มความสงบสุขของสังคม
- กลุ่มองค์กรภาครัฐ และหน่วยงานที่เกี่ยวข้องกับรัฐบาล

หลักเกณฑ์พิจารณาผลกระทบจาก

- จำนวนผู้ใช้งานที่ได้รับผลกระทบ
- ด้านความปลอดภัยในชีวิตและสุขภาพของผู้ใช้งาน
- มูลค่าความเสียหายของผู้ใช้บริการ
- กระทบต่อความมั่นคงและสงบเรียบร้อย

หลักเกณฑ์ในการพิจารณาแบ่งระดับ ความสำคัญในการปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัย 4 ด้าน ได้แก่

1. ด้านบุคลากรที่จะได้รับผลกระทบ

- กระทบต่อผู้ใช้จำนวนประมาณน้อยกว่า 10,000 คน จัดว่าเป็นระดับ Low
- กระทบต่อผู้ใช้จำนวนประมาณ 10,000 – 100,000 คน จัดว่าเป็น Moderate
- กระทบผู้ใช้จำนวนประมาณมากกว่า 100,000 คน จัดว่าเป็นระดับ High

2. ด้านความปลอดภัยในชีวิตและสุขภาพของผู้ใช้งาน

- ไม่ได้รับผลกระทบด้านความเจ็บป่วยจัดเป็นระดับ Low
- หากบาดเจ็บ หรือ ป่วย 1 คน จัดเป็นระดับ Moderate
- หากเสียชีวิตเพียง 1 คน จัดเป็นระดับ High

หลักเกณฑ์ในการพิจารณาแบ่งระดับ ความสำคัญในการปฏิบัติตามมาตรฐานด้านความมั่นคงปลอดภัย 4 ด้าน ได้แก่

3. ด้านมูลค่าความเสียหายโดยตรงของผู้ใช้บริการ

- หากเสียหายต่อธุรกิจต่อวันมูลค่าประมาณ 1 ล้านบาท จัดเป็นระดับ Low
- หากเสียหายทางธุรกิจต่อวันมูลค่าระหว่างประมาณ 1 - 100 ล้านบาทจัดเป็นระดับ Moderate
- หากเสียหายทางธุรกิจต่อวันมูลค่าเกินกว่า 100 ล้านบาท จัดเป็นระดับ High

4. ด้านผลกระทบทางด้านความมั่นคงและความสงบเรียบร้อยของประเทศ

- มีผลกระทบ
- ไม่มีผลกระทบ

- ISO/IEC 27001:2005

  Specification for Information Security Management

- ISO/IEC 17799:2005

  Code of Practice for Information Security Management

หลักการพื้นฐานที่ต้องคำนึงถึง (ม.๑๐)

- การรักษาความลับ (confidentiality)
- การรักษาความครบถ้วน (integrity)
- การรักษาสภาพพร้อมใช้งาน (availability)

การปฏิบัติตามนโยบายและแนวปฏิบัติ (ม. ๑๐)

- การควบคุมการปฏิบัติงาน
- การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

วิธีการแบบปลอดภัยมี ๓ ระดับ (ม.๔)

(๑) ระดับเคร่งครัด

(๒) ระดับกลาง

(๓) ระดับพื้นฐาน

ทั้งนี้ ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ประกาศกำหนด (ม.๖)

มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (ม. ๗)

(๑) การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

(๒) การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งภายในและภายนอกหน่วยงานหรือองค์กร

(๓) การบริหารจัดการทรัพย์สินสารสนเทศ

(๔) การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

(๕) การสร้างความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม

(๖) การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๗) การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

(๘) การจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๙) การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

(๑๐) การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

(๑๑) การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการใด ๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

มาตรา 35

การดำเนินการใดๆ ตามกฎหมาย กับหน่วยงานของรัฐ หรือ
(เช่น คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน เป็นต้น) โดยหน่วยงานของรัฐ

เมื่อได้ปฏิบัติตาม

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

- ให้นำพรบ. ธุรกรรมทางอิเล็กทรอนิกส์ฯ มาใช้บังคับ และ
- **ให้ถือว่ามีผลชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามที่กฎหมายในเรื่องนั้นกำหนด**

หลักการสำคัญของพระราชกฤษฎีกา

เจตนารมณ์ เพื่อให้หน่วยงานของรัฐได้ใช้วิธีการทางอิเล็กทรอนิกส์ภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน จึงต้องมีการกำหนดหลักเกณฑ์ และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐขึ้น

สาระสำคัญในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

- เกณฑ์มาตรฐานในการทำเอกสารในรูปข้อมูลอิเล็กทรอนิกส์
- **การจัดทำนโยบายความมั่นคงปลอดภัย** (Information Security)
- การจัดทำนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)

พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

ความเป็นมา : ตราขึ้นใช้บังคับ โดยมีสถานะเป็นกฎหมายลูกหรือกฎหมายลำดับรองของกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

ผลการบังคับใช้ : ทำให้การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐมีผลทางกฎหมาย

หน่วยงานที่ต้องปฏิบัติตาม พ.ร.ฎ. : หน่วยงานของรัฐ

ความจำเป็น : เพื่อพัฒนาการทำธุรกรรมทางออนไลน์ภาครัฐให้อยู่ภายใต้มาตรฐาน หรือ ทิศทางเดียวกัน

ความหมายของหน่วยงานของรัฐ

"หน่วยงานของรัฐ" ในความหมายตาม พ.ร.บ.ธุรกรรมฯ มาตรา 4 ได้แก่

1. กระทรวง ทบวง กรม ส่วนราชการ ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น

2. รัฐวิสาหกิจที่ตั้งขึ้นโดย พ.ร.บ. หรือพ.ร.ฎ.

3. นิติบุคคล คณะบุคคล หรือบุคคล ซึ่งมีอำนาจหน้าที่ดำเนินงานของรัฐไม่ว่าในการใดๆ เช่น **มหาวิทยาลัย** เป็นต้น

มาตรา ๓ การจัดทำเอกสารในรูปข้อมูลอิเล็กทรอนิกส์

การทำระบบเอกสารในรูปข้อมูลอิเล็กทรอนิกส์ ต้อง

(1) รูปแบบที่เหมาะสมของเอกสาร โดยต้องสามารถแสดงหรืออ้างอิงได้ในภายหลัง และมีข้อความครบถ้วน (เพื่อให้เป็นไปในแนวทางเดียวกัน)

(2) กำหนดระยะเวลาเริ่มต้น & สิ้นสุด ในการยื่นเอกสาร โดยให้ยึดตามวันและเวลาของหน่วยงานของรัฐนั้นเป็นหลัก จึงอาจจะต้องมีการตั้งนาฬิกาของระบบคอมพิวเตอร์ให้ตรงกัน เช่น ตามเวลาของกรมอุทกศาสตร์กองทัพเรือ (เพื่อประโยชน์...ผลของสัญญา, สิทธิ, หน้าที่, ดอกเบี้ย, การสิ้นสุดของสัญญา, อายุความ)

(3) ต้องกำหนดวิธีการระบุตัวบุคคล & ลายมือชื่ออิเล็กทรอนิกส์ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความข้อมูลนั้น (เพื่อประโยชน์...ผลผูกพันทางกฎหมาย)

(4) กำหนดวิธีการตอบแจ้งการรับเพื่อเป็นหลักฐานว่ามีการทำธุรกรรมทางอิเล็กทรอนิกส์แล้ว (เพื่อประโยชน์ & ความชัดเจน & ลดข้อโต้แย้งเรื่องการส่ง & รับ)

มาตรา 6 การจัดทำแนวนโยบาย/แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

ในกรณีที่มีการรวบรวม, จัดเก็บ, ใช้, เผยแพร่ข้อมูล หรือข้อเท็จจริง ทำให้ระบุตัวบุคคลได้ ไม่ว่าทางตรง หรือทางอ้อม อันกระทบต่อสิทธิขั้นพื้นฐานของประชาชน หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 5 การจัดทำแนวนโยบาย/แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

การจัดทำแนวนโยบาย/แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย อย่างน้อย ดังนี้

(1) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(2) การสำรองข้อมูล & สภาพพร้อมใช้งาน & ทำแผนฉุกเฉิน

(3) การตรวจสอบ & ประเมินความเสี่ยงอย่างสม่ำเสมอ

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

วันใช้บังคับ (ข้อ ๑๖)

- ๒๔ มิถุนายน ๒๕๕๓

ที่มา :

มาตรา ๕ พรฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

"หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้"

แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- **ทำเป็นลายลักษณ์อักษร**
- **ได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย**
- **เนื้อหาต้องประกอบด้วย**

- การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

- การจัดให้มีระบบสารสนเทศและระบบสำรองซึ่งอยู่ในสภาพพร้อมใช้งาน

- การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินเพื่อให้สามารถใช้งานได้ตามปกติอย่างต่อเนื่อง

- การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ต้องประกอบด้วย**กระบวนการ** ดังนี้

(๑) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

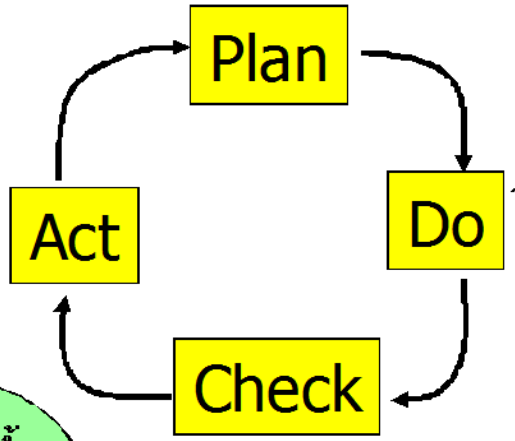
(๒) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

(๓) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติให้ชัดเจน

(๔) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

วงจร PDCA

ตารางการวิเคราะห์และบริหารจัดการความเสี่ยง



ปฏิบัติตามมาตรการในตารางการบริหารจัดการความเสี่ยง

- สร้าง Awareness เพิ่มเติมให้บางหน่วยงานที่ติดไวรัส
- หากไม่ทำการติดตั้ง ต้องกำหนดมาตรการที่เข้มงวดมากขึ้น
- ดำเนินการลงโทษผู้ละเมิดนโยบายเพื่อเป็นตัวอย่างให้พนักงานคนอื่นเห็นความสำคัญของการปฏิบัติตามนโยบายอย่างเคร่งครัด

- ตรวจสอบว่าโปรแกรมป้องกันไวรัสทำงานปกติหรือไม่
- ตรวจดูสถิติไวรัสในองค์กรว่าอยู่ในระดับใด
- ผู้ใช้ได้ติดตั้งซอฟต์แวร์ป้องกันไวรัสหรือไม่
- ผู้ใช้ปฏิบัติตามนโยบายป้องกันไวรัสหรือไม่

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ”

(๑) มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control)

(๒) มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control)

(๓) มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) และการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training)

(๔) มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน(user responsibilities)

(๕) มีการควบคุมการเข้าถึงเครือข่าย (network access control)

(๖) มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

(๗) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control)

การเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) (ข้อ ๕)

- หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

- ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ

- หน่วยงานของรัฐต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) (ข้อ ๖)

- การควบคุมการเข้าถึงสารสนเทศ และ
- การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) และการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) (ข้อ ๗)

- สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักถึงภัยและผลกระทบจากการใช้งานโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์
- การลงทะเบียนผู้ใช้งาน (user registration)
- การบริหารจัดการสิทธิของผู้ใช้งาน (user management)
- การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management)
- การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights)

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) (ข้อ ๘)

- การใช้งานรหัสผ่าน (password use)
- การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์
- การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy)
- ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

การควบคุมการเข้าถึงเครือข่าย (network access control) (ข้อ ๙)

- การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections)
- การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks)
- การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection)
- การแบ่งแยกเครือข่าย (segregation in networks)
- การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control)
- การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control)

การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) (ข้อ ๑๐)

- การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย
- การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication)
- การบริหารจัดการรหัสผ่าน (password management system)
- การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities)
- เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)
- การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time)

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) (ข้อ ๑๑)

- การจำกัดการเข้าถึงสารสนเทศ (information access restriction)
- ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)
- การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่
- การปฏิบัติงานจากภายนอกสำนักงาน (teleworking)

“การจัดระบบสำรองซึ่งอยู่ในสภาพพร้อมใช้งาน และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน”

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

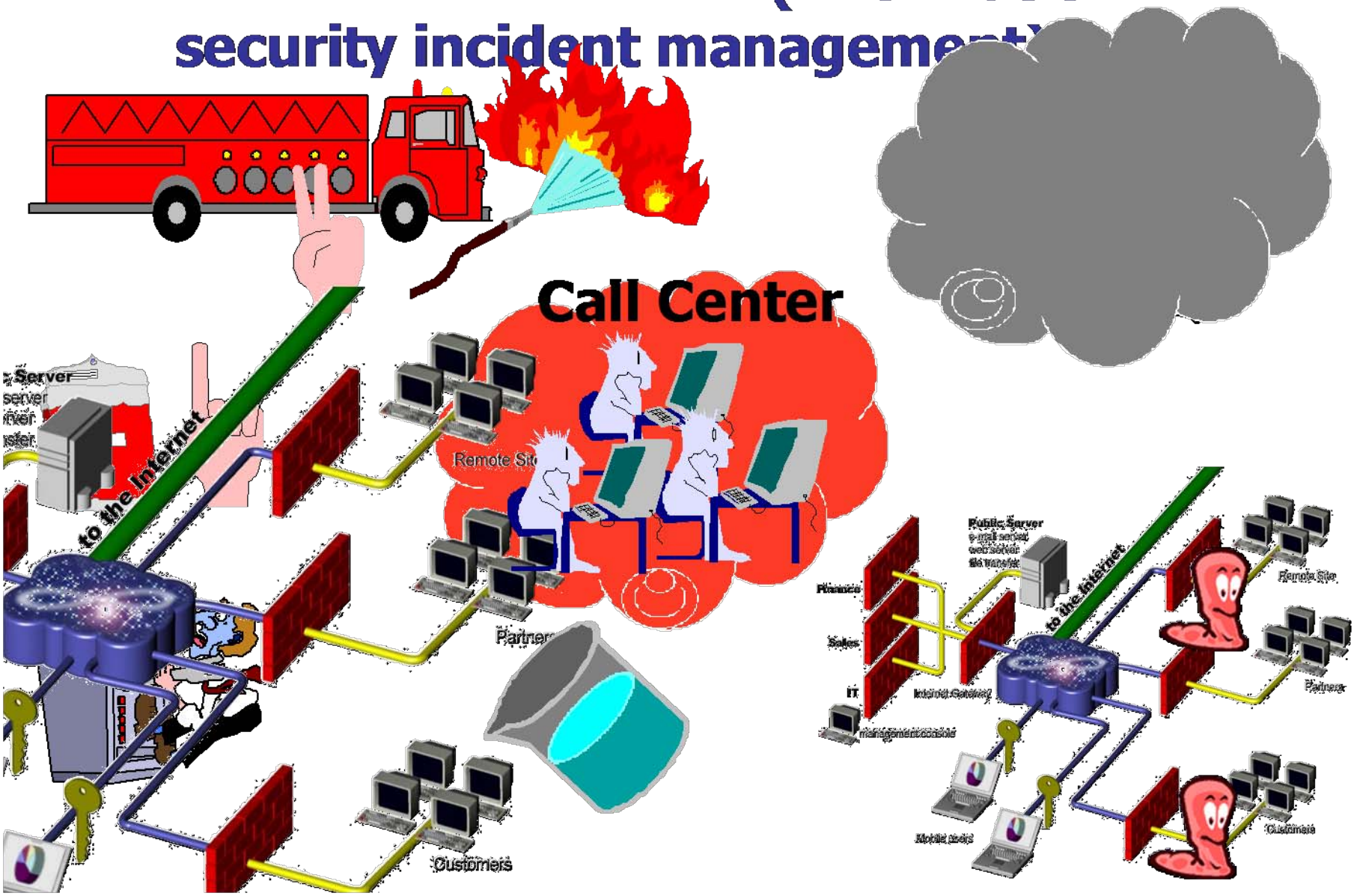
(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

(๕) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

การรับมือกับเหตุการณ์ละเมินเหตุการณ์ความปลอดภัยคอมพิวเตอร์ (information security incident management)



“การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ”

(๑) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

“การกำหนดความรับผิดชอบที่ชัดเจน”

ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ทั้งนี้ ให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ขอบคุณคะ