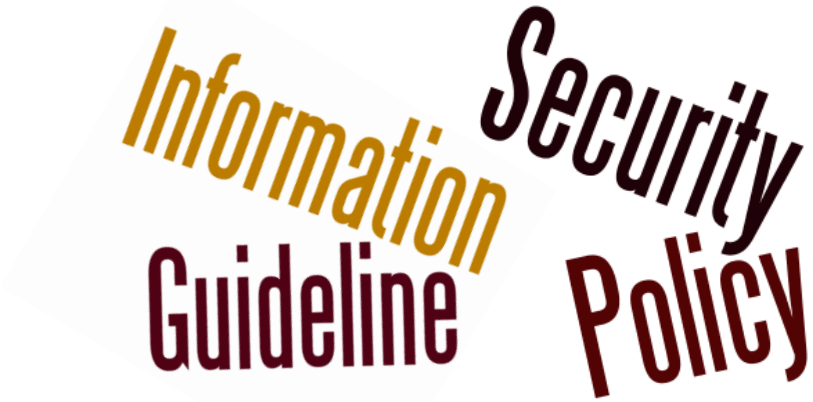


แนวทางการสร้าง นโยบายความมั่นคงปลอดภัยสารสนเทศ ให้นำไปใช้งานได้จริง

ดร.ชาลี วรกุลพิพัฒน์
CISSP, CISA
ห้องปฏิบัติการวิจัยความมั่นคงปลอดภัยไซเบอร์
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
Chalee.vorakulpipat@nectec.or.th

ประวัติวิทยากร

ดร.ชาลี วรกุลพิพัฒน์

- ประวัติการศึกษา
  - PhD (Information Systems) University of Salford ประเทศอังกฤษ
  - วท.ม. (เทคโนโลยีสารสนเทศ) มหาวิทยาลัยเกษตรศาสตร์
  - วศ.บ. (อิเล็กทรอนิกส์) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- ประวัติการทำงาน
  - หัวหน้าห้องปฏิบัติการความมั่นคงปลอดภัยไซเบอร์

    ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) (2540-ปัจจุบัน)
  - อนุกรรมการ ในคณะอนุกรรมการความมั่นคงปลอดภัย ภายใต้คณะกรรมการธุรกรรมอิเล็กทรอนิกส์ (2552-ปัจจุบัน)
  - หัวหน้าโครงการ ThaiCERT (2553-2554)
  - อาจารย์พิเศษ (เกษตรศาสตร์, ศรีปทุม, ธุรกิจบัณฑิตย์, พระนครเหนือ)
  - วิทยากรบรรยายพิเศษให้หน่วยงานภาครัฐและเอกชน

ประวัติวิทยากร

- Certificate: CISSP, CISA, IRCA:ISMS Lead Auditor ISO/IEC 27001
- รางวัลและเกียรติยศ
  - NECTEC Star 3 ครั้ง (2553,2555,2556)
  - รางวัลแนวคิดวิจัยและพัฒนา (ชมเชย) กสท โทรคมนาคม ในงานวิจัย Green Email: อีเมล์ไร้สแปม 2554
  - รางวัลวิทยานิพนธ์ดีเยี่ยม (ชนะเลิศ) สาขาเทคโนโลยีสารสนเทศและนิเทศศาสตร์ สภาวิจัยแห่งชาติ 2552
  - Outstanding Paper Award (Highly Commended), Journal of Knowledge Management 2552
  - Featured Student, Informatics Research Institute, University of Salford 2549
  - ทุน ก.พ. (กระทรวงวิทย์) ศึกษาต่อในระดับปริญญาเอก 2547
- บทความวิชาการ นานาชาติ 30 บทความ ในประเทศ 6 บทความ
- แต่งหนังสือ “UML ภาษามาตรฐานเพื่อผู้พัฒนาซอฟต์แวร์” ซีเอ็ดยูเคชัน

กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์

- กำหนดฐานความผิดที่เกิดจากการใช้ ระบบคอมพิวเตอร์และใช้คอมพิวเตอร์ เป็นเครื่องมือในการกระทำผิด

ใช้จับผู้ร้ายได้หรือไม่

- ปกติการลงโทษตามกฎหมายอาญาจะต้อง ครบองค์ประกอบความผิดในฐานความผิดนั้นๆ
- การขโมยข้อมูลคอมพิวเตอร์มีความต่างจาก การขโมยสิ่งของอื่นๆ
- ดังนั้นจึงต้องจัดการด้วยกฎหมายเฉพาะ

กฎหมายสำหรับหน่วยงานภาครัฐ

- เนื่องจากเทคโนโลยีก้าวไปอย่างรวดเร็ว และหน่วยงานต่างๆ อาจใช้เทคโนโลยี ซอฟต์แวร์ ฮาร์ดแวร์ที่แตกต่างกันในการ บริการประชาชน
- จึงต้องกำหนดวิธีการทางอิเล็กทรอนิกส์ภาย ใต้มาตรฐานเดียวกันและเป็นไปในทิศทาง เดียวกัน
- ต้องคำนึงถึงความพร้อมของแต่ละหน่วยงาน

ประกาศที่เกี่ยวข้อง

- แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- แนวนโนบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
- นอกจากนี้กฎหมายยังกำหนดให้หน่วยงาน ภาครัฐ จัดทำเอกสารอิเล็กทรอนิกส์ในรูปแบบ ที่เหมาะสม

ที่มา

- จากพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔
- มาตรา ๒๕ ธุรกรรมทางอิเล็กทรอนิกส์ใดที่ได้กระทำตามวิธีการแบบปลอดภัยที่กำหนดใน พระราชกฤษฎีกา ให้สันนิษฐานว่าเป็นวิธีการที่ เชื่อถือได้

ที่มา

- พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙
- มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการ ทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดย หน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้
- แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

พ.ร.ฎ.ธุรกรรมอิเล็กทรอนิกส์

- (๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ
- (๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของ สารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำ แผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถ ดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้ สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง
- (๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

พ.ร.ฎ.ธุรกรรมอิเล็กทรอนิกส์

- มาตรา ๖ ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้ สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย

พ.ร.ฎ.ธุรกรรมอิเล็กทรอนิกส์

- มาตรา ๗ แนวนโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือ หน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลบังคับได้
- หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนด อย่างสม่ำเสมอ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ประกอบไปด้วย 3 ส่วนหลักๆ

- การควบคุมการเข้าถึง (Access Control)
- การสำรองข้อมูล (Backup)
- การตรวจประเมิน (Assessment)

แบบประเมินตนเอง

- เป็นไปตามแต่ละข้อในแนวนโยบายและแนวปฏิบัติฯ
- ส่งให้สำนักธุรกรรมอิเล็กทรอนิกส์

ตัวอย่างแบบประเมินตนเอง

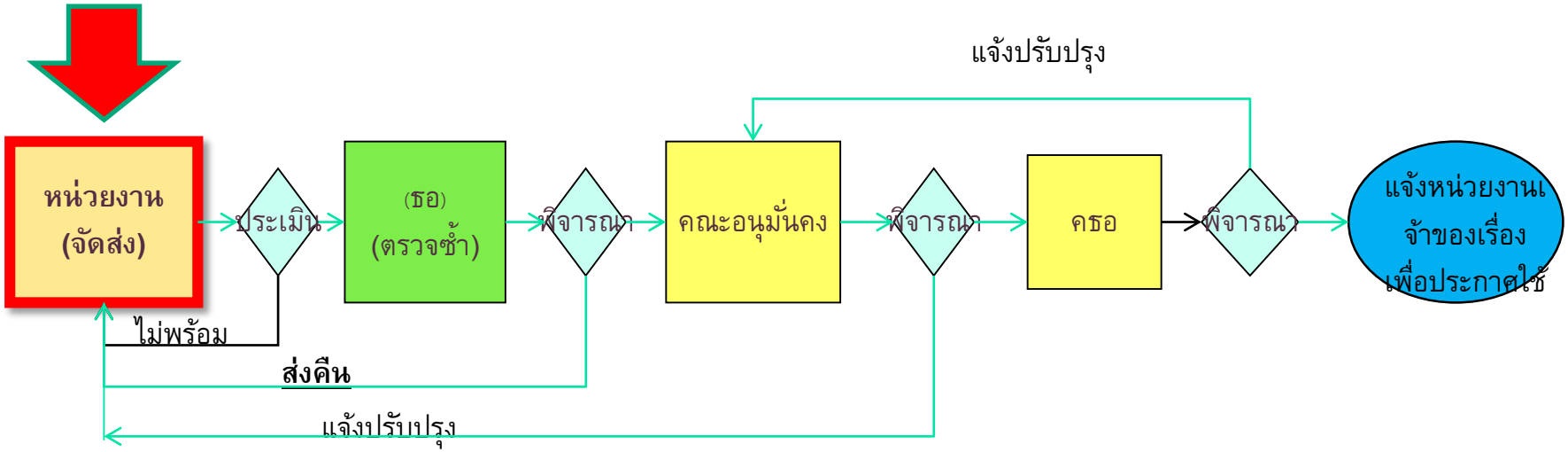
(ร่าง) แบบประเมินประกอบการพิจารณาการดำเนินงานตาม
แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ของหน่วยงานภาครัฐ
ตามมาตรา 7 ใน พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

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

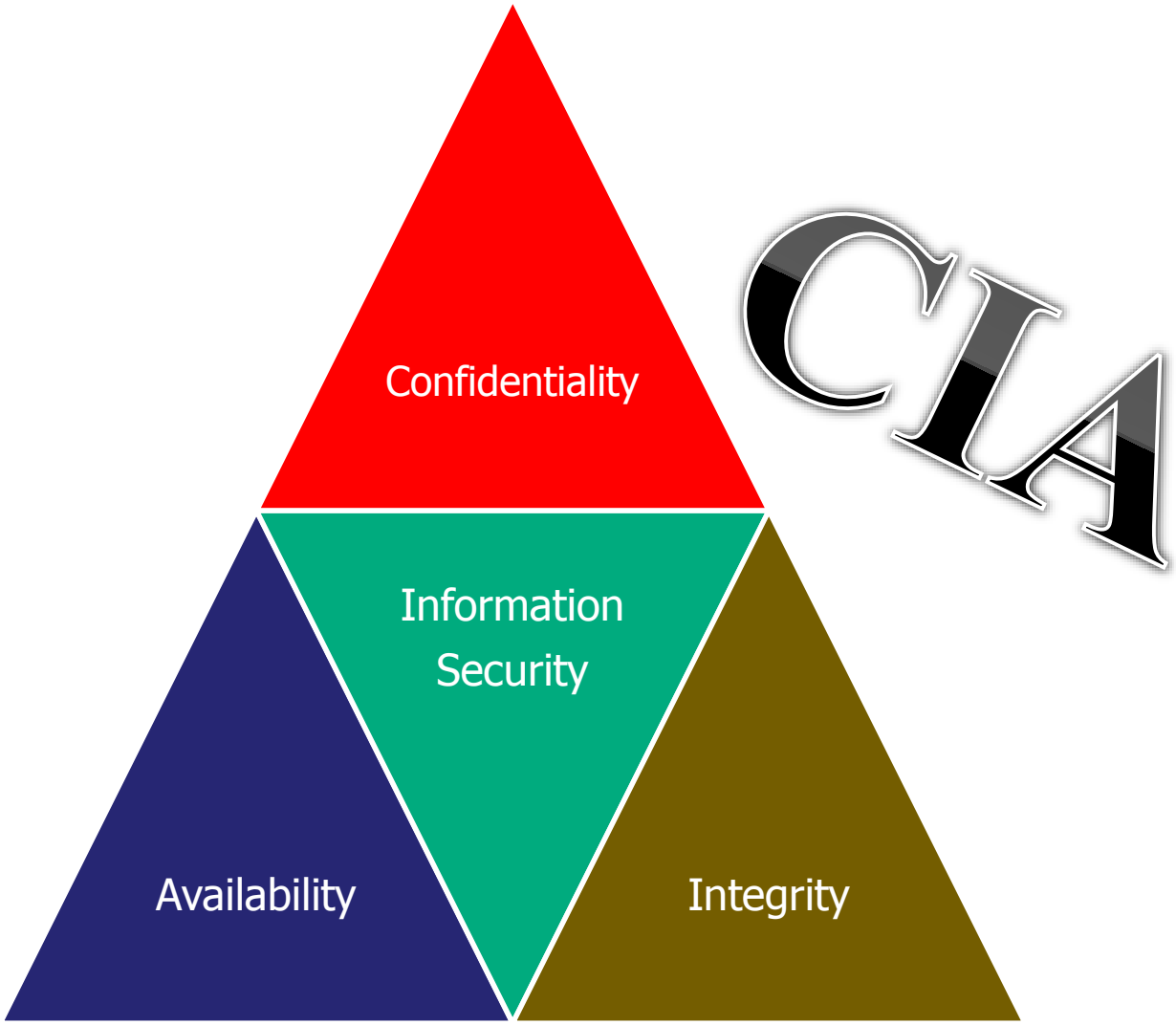
หมายเหตุ : กรณีที่กรรมการธุรกรรมทางอิเล็กทรอนิกส์ หรืออนุกรรมการมีความเกี่ยวข้องกับข้อเสนอที่กำลังพิจารณา ต้องแสดงตนเพื่อหลีกเลี่ยงปัญหาการมีผลประโยชน์ทับซ้อน (Conflicts of Interest)

ข้อ	แนวนโยบาย / และแนวปฏิบัติ (ประกาศของคณะกรรมการ)	หน่วยงานประเมินตนเอง		ความเห็นจาก รอ. เห็นด้วย/ไม่เห็นด้วย	ความเห็นจาก อนุกรรมการมั่นคงฯ
		ผ่าน/ไม่ผ่าน	อ้างอิงหน้า... / ระบุเหตุผล (ถ้ามี)		
๑	**คำนิยาม**				
	(๑) ผู้ใช้งาน				
	(๒) สิทธิของผู้ใช้งาน				
	(๓) สินทรัพย์				
	(๔) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ				
	(๕) ความมั่นคงปลอดภัยด้านสารสนเทศ				
	(๖) เหตุการณ์ด้านความมั่นคงปลอดภัย				
	(๗) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด				
	(๘) คำนิยามอื่น ๆ ตามความต้องการขององค์กร				
๒	**หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้**				
	(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ				
	(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง				
	(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ				

ขั้นตอนการพิจารณา



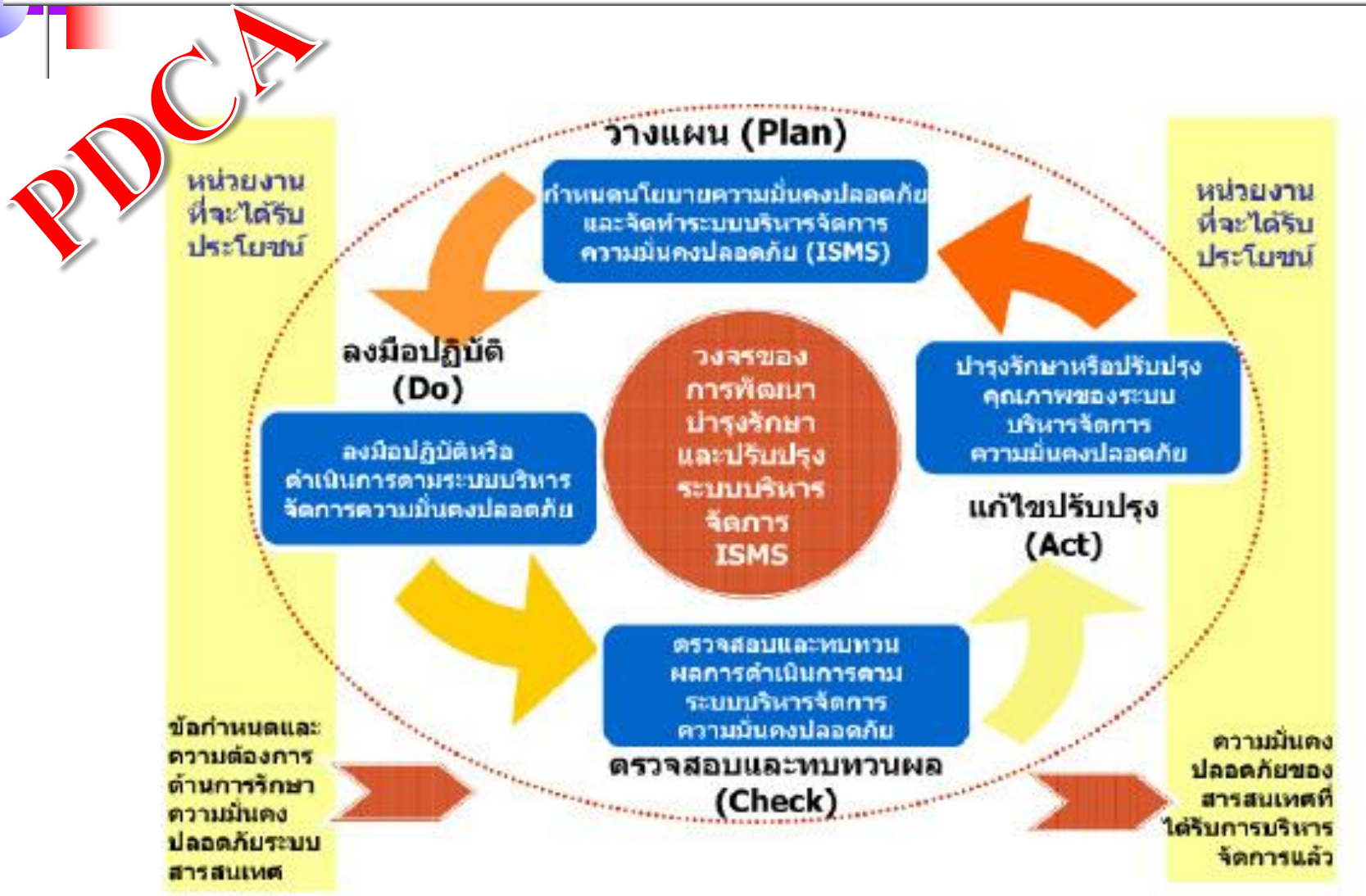
C.I.A. ในเรื่องความมั่นคงปลอดภัย



มาตรฐานความมั่นคงปลอดภัยสารสนเทศ

- ISO/IEC 27001 → Controls
- ISO/IEC 27002 → Controls + Implementation Guide

ระบบบริหารจัดการความปลอดภัยสำหรับสารสนเทศ



หน้าที่ความรับผิดชอบของผู้บริหาร

- การให้ความสำคัญในการบริหารจัดการ
- การบริหารจัดการทรัพยากรที่จำเป็นและการอบรม

การตรวจสอบภายใน

- การทำ Internal Audit
- องค์กรควรดำเนินการตรวจสอบภายในตามรอบระยะเวลาที่กำหนดไว้เพื่อตรวจสอบว่า วัตถุประสงค์ มาตรการ กระบวนการ และขั้นตอนปฏิบัติของระบบบริหารจัดการความมั่นคงปลอดภัย:
  - สอดคล้องกับข้อกำหนดในมาตรฐานฉบับนี้และกฎหมาย ข้อกำหนดอื่นๆ ที่เกี่ยวข้องหรือไม่
  - สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยที่กำหนดไว้หรือไม่
  - ได้ลงมือปฏิบัติและบำรุงรักษาอย่างสัมฤทธิ์ผลหรือไม่
  - เป็นไปตามที่คาดหมายหรือไม่
- ระบุหน้าที่ความรับผิดชอบอย่างเป็นลายลักษณ์อักษร

การทบทวนระบบ ISMS โดยผู้บริหาร

- การทำ Management Review
- ผู้บริหารจะต้องทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยตามรอบระยะเวลาที่กำหนดไว้ (เช่น ปีละ 1 ครั้ง)

การบำรุงรักษาและปรับปรุงอย่างต่อเนื่อง

- ปรับปรุง
- แก้ไข
- ป้องกัน

ISO/IEC 27001 Annex A

- 11 Controls
  - Security policy
  - Organization of information security
  - Asset management
  - Human resources security
  - Physical and environmental security
  - Communications and operations management
  - Access control
  - Information systems acquisition, development and maintenance
  - Information security incident management
  - Business continuity management
  - Compliance

นโยบายความมั่นคงปลอดภัย (Security policy)

- การทำ Information Security Policy
  - นโยบายที่เป็นลายลักษณ์อักษร
  - ทบทวนนโยบายตามระยะเวลาที่กำหนดหรือมีการเปลี่ยนแปลงที่สำคัญขององค์กร

โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

- โครงสร้างภายในองค์กร
  - การให้ความสำคัญของผู้บริหาร
  - การประสานงานภายในองค์กร
  - การกำหนดหน้าที่ความรับผิดชอบ
  - กระบวนการในการอนุมัติการใช้งานอุปกรณ์ประมวลผล
  - การลงนามมิให้เปิดเผยความลับขององค์กร
  - การมีรายชื่อติดต่อกับหน่วยงานอื่น เช่น ตำรวจ, TOT
  - การมีรายชื่อติดต่อกับหน่วยงานที่มีความสนใจพิเศษเฉพาะในเรื่องเดียวกัน เช่น สมาคม,อุตสาหกรรมต่างๆ
  - การทบทวนโดยผู้ตรวจสอบอิสระ

โครงสร้างด้านความมั่นคงปลอดภัยสำหรับองค์กร (Organization of information security)

- โครงสร้างเกี่ยวกับลูกค้าหรือหน่วยงานภายนอก
  - การประเมินความเสี่ยง
  - การระบุข้อกำหนดสำหรับลูกค้าหรือผู้ใช้บริการ
  - การระบุข้อกำหนดสำหรับหน่วยงานภายนอก

การบริหารจัดการทรัพย์สินขององค์กร (Asset management)

- หน้าที่ความรับผิดชอบต่อทรัพย์สินองค์กร
  - จัดทำบัญชีทรัพย์สิน
  - ระบุผู้เป็นเจ้าของทรัพย์สิน
  - ใช้งานทรัพย์สินที่เหมาะสม
- การจัดหมวดหมู่สารสนเทศ
  - จัดตามลำดับชั้นความลับ คุณค่า ข้อกำหนดทางกฎหมาย และผลกระทบ
  - จัดทำป้ายชื่อ

ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

- ก่อนการจ้างงาน
  - กำหนดหน้าที่ความรับผิดชอบด้าน security
  - ตรวจสอบคุณสมบัติของผู้สมัคร (screening)
  - กำหนดเงื่อนไขการจ้างงาน

ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

- ระหว่างการจ้างงาน
  - กำหนดหน้าที่ความรับผิดชอบด้าน security
  - สร้างความตระหนัก อบรม
  - กระบวนการทางวินัย ลงโทษ

ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human resources security)

- สิ้นสุดหรือเปลี่ยนการจ้างงาน
  - คืนทรัพย์สิน
  - ถอดสิทธิ

การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

- บริเวณที่ต้องมี security
  - การจัดทำบริเวณล้อมรอบ
  - การควบคุมการเข้า-ออก
  - การสร้าง security ในสำนักงาน และทรัพย์สินอื่นๆ
  - การป้องกันภัยคุกคามจากภายนอก
  - การปฏิบัติงานในพื้นที่ที่มี security
  - การจัดบริเวณการเข้าถึงสำหรับบุคคลภายนอก

การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environmental security)

- Security ของอุปกรณ์
  - การจัดวางและการป้องกันของอุปกรณ์
  - ระบบและอุปกรณ์สนับสนุนการทำงาน
  - การเดินสายไฟ เคเบิล และสายอื่นๆ
  - การบำรุงรักษาอุปกรณ์
  - การป้องกันอุปกรณ์ที่ใช้งานอยู่ภายนอกสำนักงาน
  - การกำจัดอุปกรณ์หรือนำอุปกรณ์กลับมาใช้ใหม่
  - การนำอุปกรณ์ออกนอกสำนักงาน

- การกำหนดหน้าที่ความรับผิดชอบ
  - กำหนดขั้นตอนเป็นลายลักษณ์อักษร
  - ควบคุมการเปลี่ยนแปลง (change management)
  - แบ่งหน้าที่ความรับผิดชอบ (segregation of duties)
  - แยกระบบสำหรับการพัฒนา ทดสอบ และการให้บริการออกจากกัน

- การบริหารจัดการการให้บริการของหน่วยงานภายนอก
  - กำหนดให้หน่วยงานภายนอกปฏิบัติตามข้อกำหนดที่ตกลงไว้ระหว่างกัน
  - ตรวจสอบการให้บริการของหน่วยงานภายนอกอย่างสม่ำเสมอ (monitoring)
  - บริหารจัดการการเปลี่ยนแปลงในการให้บริการ

- การวางแผนและการยอมรับระบบสารสนเทศ (planning and acceptance)
  - วางแผนตามความต้องการ
  - มีมาตรการหรือขั้นตอนในการยอมรับระบบนั้นๆ มาใช้
- การป้องกันโปรแกรมไม่ประสงค์ดี
  - มีมาตรการป้องกัน กู้คืน
  - ป้องกันโปรแกรมประเภท mobile code เช่น Java applet, JavaScript, ActiveX, Flash

- การสำรองข้อมูล (backup)
  - มีการสำรองและทดสอบการสำรองอย่างสม่ำเสมอ
- บริหารเครือข่าย (Network security management)
  - มีมาตรการทางเครือข่าย
  - กำหนดคุณสมบัติระดับการให้บริการและมีข้อกำหนดในการบริหารจัดการเครือข่ายที่องค์กรใช้บริการอยู่และต้องกำหนดในข้อตกลงในการให้บริการด้วย

- การจัดการสื่อบันทึกข้อมูล (Media Handling)
  - บริหารจัดการสื่อที่เคลื่อนย้ายได้ (Removable media)
  - กำจัดสื่อบันทึกข้อมูล เช่น ทุบทิ้ง, Degaussing
  - มีขั้นตอนปฏิบัติการจัดการข้อมูลข้างใน
  - กำหนดมาตรการป้องกันการเข้าถึงข้อมูลในสื่อ

- การแลกเปลี่ยนสารสนเทศ (Exchange)
  - มีนโยบายและแลกเปลี่ยน
  - จัดทำข้อตกลงในการแลกเปลี่ยนเป็นลายลักษณ์อักษร
  - มีมาตรการการนำสื่อบันทึกข้อมูลออกไปข้างนอก
  - มีมาตรการการส่งข้อมูลทางอิเล็กทรอนิกส์ เช่น ส่ง email
  - มีมาตรการที่เกี่ยวกับข้อมูลและขั้นตอนทางธุรกิจ

- การสร้าง security ใน E-commerce
  - มีมาตรการป้องกันใน E-commerce เช่น การเปลี่ยนแปลงเว็บไซต์โดยไม่ได้รับอนุญาต
  - มีมาตรการในการทำธุรกรรมออนไลน์
  - ให้ข้อมูลมีความถูกต้องและพร้อมใช้งานเสมอ

- การเฝ้าระวัง (Monitoring)
  - บันทึกเหตุการณ์ตลอดเวลาใน Log (Audit Logging)
  - ตรวจสอบการใช้งาน (Monitoring)
  - ป้องกันข้อมูลใน Log เช่นไม่ให้ถูกแก้ไข
  - บันทึก Log กิจกรรมของเจ้าหน้าที่ด้วย
  - บันทึกเหตุการณ์ข้อผิดพลาด (Fault Logging)
  - ตั้งเวลาแต่ละเครื่องให้ตรงกัน (Clock synchronizing)

การควบคุมการเข้าถึง (Access Control)

- มีข้อกำหนดทางธุรกิจ (Business Requirement)
  - มีนโยบายการเข้าถึงเป็นลายลักษณ์อักษรและปรับปรุงอย่างสม่ำเสมอ
- บริหารการเข้าถึงของผู้ใช้ (User Access)
  - มีขั้นตอนการลงทะเบียนพนักงาน เช่น เข้าใหม่, ลาออก, เปลี่ยนตำแหน่ง
  - จัดการสิทธิการใช้งานระบบ
  - จัดการรหัสผ่าน
  - ทบทวนสิทธิ

การควบคุมการเข้าถึง (Access Control)

- กำหนดหน้าที่ความรับผิดชอบของผู้ใช้
  - วิธีปฏิบัติในการใช้รหัสผ่าน
  - มีวิธีป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล
  - มีนโยบายควบคุมการไม่ทิ้งทรัพย์สินในที่ที่ไม่ปลอดภัย

การควบคุมการเข้าถึง (Access Control)

- ควบคุมการเข้าถึงเครือข่าย (Network access control)
  - มีนโยบายการใช้งานเครือข่าย
  - มีการพิสูจน์ตัวตนสำหรับผู้ใช้ภายนอกองค์กร
  - มีการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย
  - มีการควบคุมการเข้าถึงและใช้งานพอร์ต
  - มีการแบ่งแยกเครือข่าย (segregation in networks)
  - มีการควบคุมการเชื่อมต่อทาเครือข่าย
  - มีการควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

การควบคุมการเข้าถึง (Access Control)

- ควบคุมการเข้าถึงระบบปฏิบัติการ
  - มีขั้นตอนการเข้าถึงระบบ (secure log-on)
  - มีการพิสูจน์ตัวตน
  - บริหารจัดการรหัสผ่าน
  - ควบคุมการใช้งานโปรแกรมยูทิลิตี้
  - ให้มีการ "หมดเวลา" การใช้งาน (session time-out)
  - ให้มีการ "หมดเวลา" การเชื่อมต่อระบบสารสนเทศ

การควบคุมการเข้าถึง (Access Control)

- ควบคุมการเข้าถึง Application และสารสนเทศ
  - จำกัดการเข้าถึง
  - แยกระบบที่มีความสำคัญสูง
- ควบคุมอุปกรณ์สื่อสารแบบพกพาและการปฏิบัติงานจากภายนอกองค์กร
  - มีนโยบายควบคุมการใช้อุปกรณ์พกพา เช่น Notebook, Smart phone, Tablet
  - ควบคุมการทำงานจากภายนอก (Teleworking)

การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

- มีการวิเคราะห์และระบุข้อกำหนดด้าน security สำหรับระบบสารสนเทศใหม่หรือระบบที่ปรับปรุงจากระบบที่มีอยู่แล้ว

การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

- ควบคุมให้การประมวลผล Application มีความถูกต้อง ไม่ผิดพลาด
  - ตรวจสอบข้อมูลเข้า (Input validation)
  - ตรวจสอบข้อมูลที่อยู่ในระหว่างการประมวลผล
  - ตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูล
  - ตรวจสอบข้อมูลนำออก (Output validation)

การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

- การเข้ารหัสลับของข้อมูล (Cryptographic control)
  - มีนโยบายการเข้ารหัสลับ
  - มีการบริหารจัดการกุญแจเข้ารหัสลับข้อมูล (Key management)

การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

- การสร้าง security ให้กับไฟล์
  - ควบคุมการติดตั้งซอฟต์แวร์ลงระบบ
  - ป้องกันข้อมูลที่ใช้ในการทดสอบ
  - ควบคุมการเข้าถึง source code

การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

- การสร้าง security ในการพัฒนาระบบและการทำงานสนับสนุนอื่นๆ
  - มีขั้นตอนการควบคุมการแก้ไขระบบ
  - มีการตรวจสอบการทำงานระบบภายหลังการเปลี่ยนแปลง
  - จำกัดการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ที่มาจากผู้ผลิต
  - ป้องกันข้อมูลรั่วไหล (Information leakage)
  - มีมาตรการควบคุมการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก

การจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ (Information systems acquisition, development and maintenance)

- การบริหารจัดการช่องโหว่ในฮาร์ดแวร์และซอฟต์แวร์
  - มีมาตรการควบคุมทางเทคนิค
  - ประเมินความเสี่ยง

การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยขององค์กร (Information security incident management)

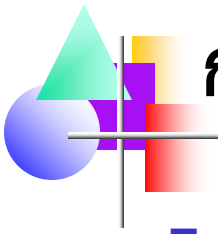
- รายงานเหตุการณ์และจุดอ่อนด้าน security
  - มีช่องทางให้รายงานเหตุการณ์อย่างทันท่วงที
  - ต้องบันทึก/รายงานจุดอ่อนที่พบหรือสงสัย
- บริหารจัดการและปรับปรุงแก้ไขต่อเหตุการณ์ที่เกิดขึ้น
  - กำหนดหน้าที่และผู้รับผิดชอบ
  - เรียนรู้จากเหตุการณ์ผ่านการจดบันทึก จะได้เตรียมการในการป้องกันในอนาคต
  - รวบรวมหลักฐาน

การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)

- บริหารความต่อเนื่องในการดำเนินงานขององค์กร
  - กำหนดกระบวนการไม่ให้องค์กรหยุดชะงัก
  - ประเมินความเสี่ยงในการบริหารความต่อเนื่อง
  - จัดทำแผนการดำเนินการที่ทำให้ธุรกิจเดินต่อได้
  - กำหนด Framework
  - ทดสอบและปรับปรุงแผนเป็นระยะๆ

การปฏิบัติตามข้อกำหนด (Compliance)

- ปฏิบัติตามข้อกฎหมาย
  - ระบุข้อกำหนดต่างๆ ที่มีผลทางกฎหมาย
  - ป้องกันการละเมิดสิทธิและทรัพย์สินทางปัญญา
  - ปกป้องข้อมูลขององค์กรที่อาจส่งผลทางกฎหมาย
  - ป้องกันข้อมูลส่วนตัว (Data privacy and protection of personal information)
  - การป้องกันการใช้งานอุปกรณ์ผิดวัตถุประสงค์หรือโดยไม่ได้รับอนุญาต
  - การใช้มาตรการเข้ารหัสลับที่สอดคล้องกับกฎหมาย

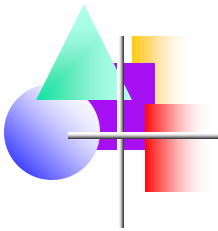


การปฏิบัติตามข้อกำหนด (Compliance)

- ปฏิบัติตามนโยบายและข้อกำหนดทางเทคนิค
  - ควบคุมให้ผู้ใต้บังคับบัญชาปฏิบัติตาม
  - ตรวจสอบระบบให้เป็นไปตามมาตรฐานหรือข้อกำหนดทางเทคนิค

การปฏิบัติตามข้อกำหนด (Compliance)

- การตรวจประเมินระบบสารสนเทศ (Audit)
  - ระบุข้อกำหนดและกิจกรรมในการตรวจประเมินเพื่อให้มีผลกระทบน้อยที่สุดต่อธุรกิจ
  - การป้องกันการใช้เครื่องมือตรวจประเมิน (Audit tools) ที่ผิดวัตถุประสงค์หรือเปิดเผยข้อมูลการตรวจประเมินโดยไม่ได้รับอนุญาต



ขอบคุณครับ