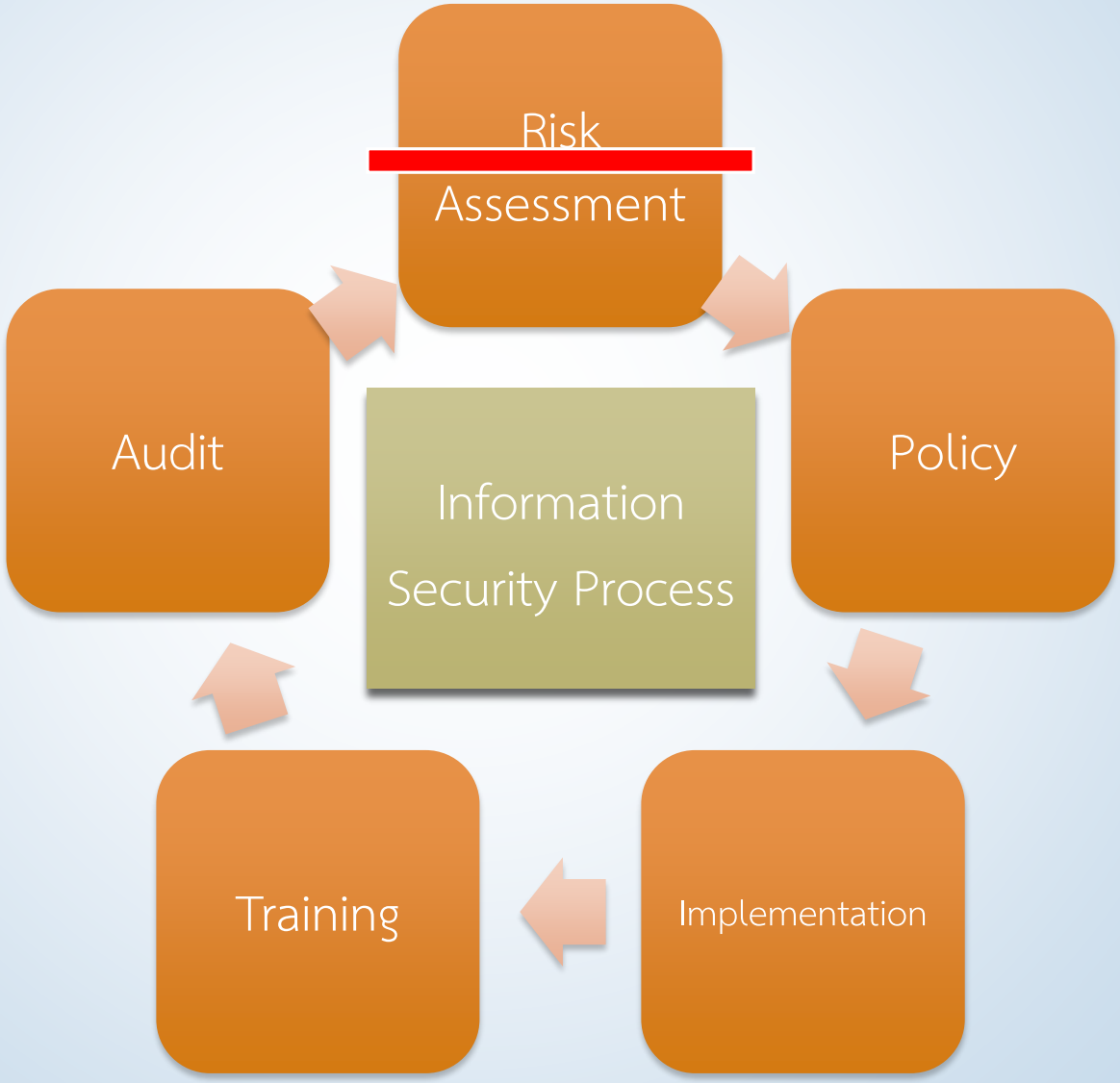
# บทที่ 2 : กระบวนการการรักษาความปลอดภัยข้อมูล Part2

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

# กระบวนการรักษาความปลอดภัยข้อมูล



# Outline

- นโยบาย (Policy)
- การติดตั้งระบบรักษาความปลอดภัย (Implementation)
- การฝึกอบรม (Training)
- การตรวจสอบ (Audit)

# นโยบาย (Policy)

- นโยบายและระเบียบปฏิบัติที่องค์กรควรมี คือ
  - นโยบายข้อมูล (Information Policy)
  - นโยบายการรักษาความปลอดภัย (Security Policy)
  - นโยบายการใช้งาน (Usage Policy)
  - นโยบายการสำรอง (Backup Policy)
  - ระเบียบปฏิบัติเกี่ยวกับการบริหารจัดการบัญชีผู้ใช้ (Account Management Procedure)
  - ระเบียบปฏิบัติเมื่อเกิดเหตุการณ์ (Incident Handling Procedure)
  - แผนการฟื้นฟูหลังภัยร้ายแรง (Disaster Recovery Plan)

# นโยบาย (Policy) : ลำดับการกำหนดนโยบาย

- ถ้าองค์กรยังไม่มีนโยบายใดๆเลย **คำถาม**คือเราจะเลือกกำหนดนโยบายใดก่อน
- **คำตอบ** คือ ขึ้นอยู่กับความเสี่ยงขององค์กรในขณะนั้น
- แต่นโยบายหนึ่งที่ควรกำหนดขึ้นในช่วงแรกๆของกระบวนการ คือ “นโยบายข้อมูล” เพราะเป็นสิ่งที่กำหนดว่าข้อมูลขององค์กรมีความสำคัญอย่างไร และจะป้องกันอย่างไร
- สามารถเขียนนโยบายหลายๆนโยบายพร้อมๆกันได้ ขึ้นอยู่กับบุคลากรที่เกี่ยวข้อง

# นโยบาย (Policy) : ปรับปรุงนโยบายที่มีอยู่แล้ว

- จำเป็นต้องปรับปรุงให้มีความทันสมัย โดยเริ่มจากการวิเคราะห์นโยบายว่ามีจุดด้อยตรงไหน
- ในกรณีที่คณะจัดทำนโยบายไม่ได้อยู่ในองค์กรแล้ว การเริ่มต้นจากศูนย์อาจเป็นสิ่งที่ง่ายกว่า

# การออกแบบและติดตั้งระบบรักษาความปลอดภัย (Implementation)

- ในการบังคับใช้นโยบายการรักษาความปลอดภัยให้ได้ผลนั้นต้องเกี่ยวข้องกับการจัดหาเครื่องมือ เทคนิค และระบบควบคุมการเข้าถึงทางกายภาพ
- อาจต้องมีการคอนฟิกระบบที่ไม่ได้อยู่ในการควบคุมเสียใหม่
- ตรวจสอบดูว่าการติดตั้งแต่ละระบบมีผลกระทบต่อระบบอื่นอย่างไร

# การออกแบบและติดตั้งระบบรักษาความปลอดภัย : ระบบรายงานการรักษาความปลอดภัย

- เป็นกลไกที่ช่วยให้ฝ่ายรักษาความปลอดภัยทราบถึงการปฏิบัติตามนโยบายของพนักงานทั่วไป และติดตามสถานภาพเกี่ยวกับจุดอ่อนในปัจจุบัน อาจใช้การรายงานด้วยมือหรือระบบอัตโนมัติก็ได้
- 1) การเฝ้าระวังการใช้งานระบบ (Monitoring)
- 2) การสแกนช่องโหว่ของระบบ
- 3) การปฏิบัติตามนโยบาย

# การออกแบบและติดตั้งระบบรักษาความปลอดภัย :

## ระบบพิสูจน์ทราบตัวตน (Authentication System)

- ใช้ตรวจสอบผู้ใช้ที่ต้องการล็อกอินเข้าใช้งานระบบหรือเครือข่าย
- ตรวจสอบการเข้าสถานที่ต้องห้าม
- ทุกระบบในองค์กรควรต้องมีระบบพิสูจน์ตัวตนด้วย
- ระบบพิสูจน์ทราบตัวตนจะมีผลกระทบกับทุกระบบขององค์กร ไม่ควรติดตั้งและใช้งานโดยที่ไม่ได้วางแผนล่วงหน้าก่อน

# การออกแบบและติดตั้งระบบรักษาความปลอดภัย : การรักษาความปลอดภัยในการใช้อินเทอร์เน็ต

- เป็นระบบที่ต้องใช้ไฟร์วอลล์และ VPN (Virtual Private Network) ซึ่งการใช้ VPN ต้องมีการเข้ารหัสข้อมูลไว้ด้วย
- การติดตั้งอาจต้องเปลี่ยนโครงสร้างของเครือข่าย
- สิ่งที่สำคัญที่สุดคือตำแหน่งที่ติดตั้งไฟร์วอลล์ ซึ่งต้องติดตั้งระหว่างอินเทอร์เน็ตและเครือข่ายภายใน การติดตั้งควรทำเมื่อออกแบบโครงสร้างพื้นฐานของเครือข่ายเสร็จสมบูรณ์แล้ว เพื่อจะได้กำหนดขนาดและประสิทธิภาพของไฟร์วอลล์ได้เหมาะสม

# การออกแบบและติดตั้งระบบรักษาความปลอดภัย : ระบบตรวจจับและป้องกันการบุกรุก

- Intrusion Detection System (IDS) เป็นระบบเตือนภัยของเครือข่าย รวมไปถึงสัญญาณเตือนกันขโมยที่ใช้สำหรับตรวจจับผู้ไม่ประสงค์ดีพยายามจะบุกรุกเข้าสถานที่ต้องห้ามด้วย
- AntiVirus เป็น IDS ที่ใช้ทรัพยากรน้อยที่สุด จึงควรติดตั้งลงในคอมพิวเตอร์ทุกเครื่อง
- การติดตั้ง IDS นั้นไม่ควรทำจนกว่าจะระบุพื้นที่ความเสี่ยงสูงได้เสียก่อน

# การออกแบบและติดตั้งระบบรักษาความปลอดภัย : การเข้ารหัสข้อมูล (Encryption)

- กลไกการเข้ารหัสข้อมูลอาจใช้สำหรับป้องกันข้อมูลในระหว่างการส่งผ่านเครือข่าย หรือระหว่างอุปกรณ์จัดเก็บข้อมูล
- สิ่งที่ควรคำนึงในการเข้ารหัสคืออาจทำให้การไหลของข้อมูลช้าลง ดังนั้นจึงไม่มีความจำเป็นที่จะต้องเข้ารหัสทุกๆข้อมูลที่มี

# การออกแบบและติดตั้งระบบรักษาความปลอดภัย : การรักษาความปลอดภัยด้านกายภาพ

- ปกติจะถูกแยกออกจากการรักษาความปลอดภัยข้อมูลหรือการสื่อสาร
- เช่น การติดตั้งระบบกล้องวงจรปิด กุญแจ การ์ดรูด เจ้าหน้าที่รักษาความปลอดภัย การกำหนดให้พนักงานทุกคนต้องติดป้ายแสดงตน เป็นต้น
- ควรพิจารณาการรักษาความปลอดภัยในพื้นที่ดาต้าเซ็นเตอร์เป็นพิเศษ เช่นระบบป้องกันต้องหนาแน่น ระบบป้องกันไฟไหม้ ระบบควบคุมอุณหภูมิ และระบบสำรองไฟฟ้าที่ดี

# การออกแบบและติดตั้งระบบรักษาความปลอดภัย : คณะทำงาน

- เมื่อมีการติดตั้งระบบป้องกันและรักษาความปลอดภัย จะต้องมีเจ้าหน้าที่ดูแลอย่างเหมาะสม บางระบบต้องมีผู้ดูแลตลอดเวลา
- การรักษาความปลอดภัยขององค์กรควรถือเป็นหน้าที่และความรับผิดชอบของพนักงานทุกคนในองค์กร

# การฝึกอบรม (Training)

- การฝึกอบรมอาจจัดเป็นการประชุม การแจงให้ทราบ หรือการตีพิมพ์ผ่านสื่อต่างๆขององค์กร โดยต้องทำควบคู่กันไปและทำเป็นประจำ
- **พนักงาน** ควรเป็นส่วนหนึ่งของการปฐมนิเทศพนักงานใหม่ด้วย
- **ผู้ดูแลระบบ** ควรปรับปรุงความรู้ให้ทันสมัยอยู่เสมอ
- **นักพัฒนาแอพพลิเคชัน** เทคนิคการเขียนโปรแกรมให้มีความปลอดภัย
- **ผู้บริหาร** ควรได้รับรายงานสถานภาพและความก้าวหน้าของโครงการติดตั้งระบบรักษาความปลอดภัย
- **คณะเจ้าหน้าที่ฝ่ายรักษาความปลอดภัย** ต้องปรับปรุงความรู้ให้ทันสมัยเพื่อจะได้สามารถให้บริการกับองค์กรได้

# การตรวจสอบ (Audit)

- เป็นขั้นตอนสุดท้ายเพื่อตรวจสอบว่ามีการฝ่าฝืนนโยบายและระเบียบปฏิบัติหรือไม่ การตรวจสอบด้านการรักษาความปลอดภัยมี 3 ประเภท
  - **การตรวจสอบการปฏิบัติตามนโยบาย**
  - **การประเมินโครงการใหม่**
  - **การทดลองเจาะระบบ (Penetration Testing)** ถ้าการเจาะระบบสำเร็จ จะทำให้ทราบว่าองค์กรมีจุดอ่อนเพิ่มขึ้นอย่างน้อยหนึ่งจุด แต่หากเจาะไม่สำเร็จก็ไม่ได้หมายความว่าระบบจะไม่มีจุดอ่อน