Information Security Policy

MS1 Thanin Muangpool

นโยบายความมั่นคงปลอดภัยของสารสนเทศและความสำคัญ

NIST (National Institute of Standard and Technology) ได้กล่าวไว้ว่า “ความสำเร็จของงานใดๆ ที่เกี่ยวข้องกับการป้องกันสารสนเทศ ขึ้นอยู่กับนโยบายที่กำหนด รวมถึงทัศนคติของฝ่ายบริหารที่มีต่อระบบความมั่นคงปลอดภัยของสารสนเทศ ในฐานะของผู้กำหนดนโยบาย จะต้องมุ่งเน้นและแสดงให้ทุกฝ่ายเห็นว่างานทางด้านความมั่นคงปลอดภัยของสารสนเทศ มีบทบาทสำคัญอย่างไรในองค์กร ดังนั้น สิ่งที่จะต้องทำอันดับแรก คือการกำหนดนโยบายความมั่นคงปลอดภัยที่มีวัตถุประสงค์เพื่อลดความเสี่ยง เพื่อให้สอดคล้องกับกฎหมาย และเพื่อรับประกันความต่อเนื่องของธุรกิจ ความสมบูรณ์ของสาสนเทศ และการปกปิดสารสนเทศที่เป็นความลับไว้”

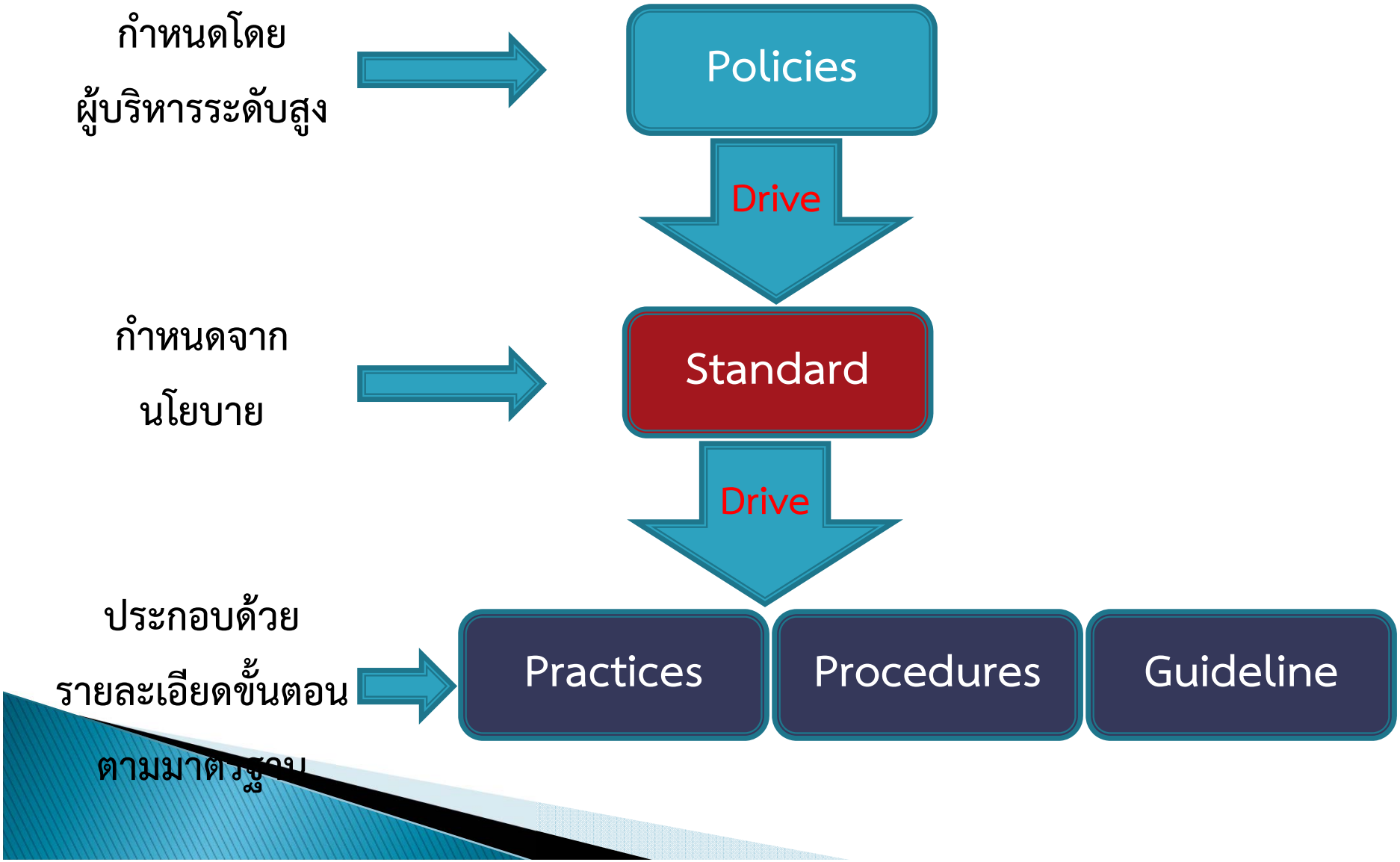
นโยบายความมั่นคงปลอดภัยของสารสนเทศและความสำคัญ

นโยบาย (Policy) คือแผนงานหรือกลุ่มของข้อปฏิบัติที่องค์กรใช้เป็นตัวกลางในการถ่ายทอดคำสั่งผู้บริหารระดับสูงไปยังบุคลากรในระดับตัดสินใจ ระดับปฏิบัติการ รวมถึงบุคลากรในหน้าที่อื่น ๆ ที่ต้องปฏิบัติตามนโยบาย

Policy จะนำไปสู่การกำหนด มาตรฐาน (Standard) ซึ่งจะนำไปสู่

- วิธีปฏิบัติ (Practice)
- ลำดับขั้นตอน (Procedure)
- แนวทาง (Guideline)

นโยบายความมั่นคงปลอดภัยของสารสนเทศและความสำคัญ



นโยบายความมั่นคงปลอดภัยของสารสนเทศและความสำคัญ

การกำหนดนโยบาย (Policy) จะต้องสอดคล้องและสนับสนุนองค์กรในด้าน

- ภารกิจ (Mission)
- วิสัยทัศน์ (Vision)
- แผนกลยุทธ์ (Strategic Plan)

ดังนั้น จึงสรุปได้ว่า

นโยบายความมั่นคงปลอดภัยของสารสนเทศ (Information Security Policy) คือ กฎข้อบังคับที่ใช้ในการป้องกันสารสนเทศขององค์กร

นโยบายความมั่นคงปลอดภัยของสารสนเทศและความสำคัญ

การกำหนดนโยบายที่ดี ควรมีลักษณะ ดังนี้

1. ไม่ขัดต่อกฎหมาย
2. สามารถใช้ในชั้นศาลได้หากจำเป็น
3. ต้องได้รับการสนับสนุนและการบริหารจัดการที่ดี
4. ต้องมีส่วนช่วยให้องค์กรประสบความสำเร็จ
5. ฝ่ายบริหารต้องมั่นใจว่ามีการกำหนดข้อได้อย่างเหมาะสม
6. ควรให้ผู้ใช้ระบบสารสนเทศมีส่วนร่วมในขั้นตอนกำหนดนโยบาย
7. จะต้องตอบสนองความต้องการขององค์กรได้อย่างแท้จริง

นโยบายความมั่นคงปลอดภัยของสารสนเทศและความสำคัญ

NIST ได้ระบุไว้ในเอกสารเผยแพร่ฉบับพิเศษ 800-14 ว่าในการกำหนดนโยบายความมั่นคงปลอดภัยของสารสนเทศที่ครบถ้วนสมบูรณ์ ทีมงานจะต้องกำหนดทั้งหมด 3 ชนิด

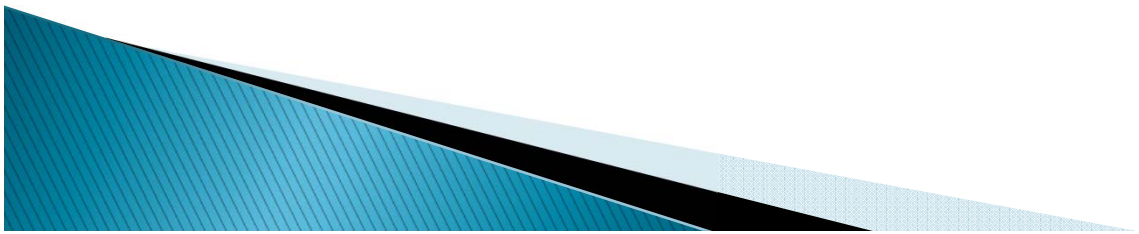
1. นโยบายความมั่นคงปลอดภัยของสารสนเทศระดับองค์กร (Enterprise Information Security Policy)
2. นโยบายความมั่นคงปลอดภัยเฉพาะเรื่อง (Issue-specific Security Policy)
3. นโยบายความมั่นคงปลอดภัยเฉพาะระบบ (System-specific Security Policy)

นโยบายความมั่นคงปลอดภัยของสารสนเทศระดับองค์กร

นโยบายความมั่นคงปลอดภัยของสารสนเทศระดับองค์กร (Enterprise Information Security Policy : EISP) คือ การกำหนดทิศทางและขอบเขตเชิงกลยุทธ์เพื่อความมั่นคงปลอดภัยขององค์กร หรืออาจเรียกว่า

- General Security Policy
- IT Security Policy
- High-level Information Security Policy
- Information security Policy

ผู้ที่ทำหน้าที่กำหนดนโยบายได้แก่**ผู้บริหารระดับสูง หรือระดับอาวุโส**



นโยบายความมั่นคงปลอดภัยของสารสนเทศระดับองค์กร

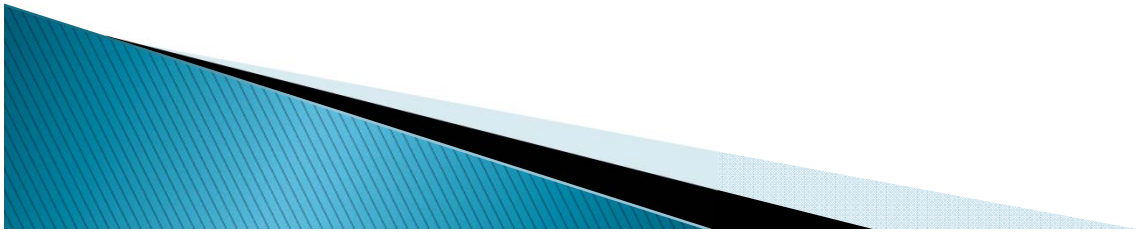
EISP มีองค์ประองประกอบ ดังนี้

1. ประกาศวัตถุประสงค์
2. องค์ประกอบความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ
   - การป้องกันความลับ (Confidentiality)
   - ความถูกต้องสมบูรณ์ (Integrity)
   - ความพร้อมใช้งาน (Availability)
3. ความจำเป็นที่ต้องมีความมั่นคงปลอดภัย
4. บทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัย
5. อ้างอิงมาตรฐานและแนวทางอื่น ๆ

นโยบายความมั่นคงปลอดภัยของสารสนเทศเฉพาะเรื่อง

นโยบายความมั่นคงปลอดภัยเฉพาะเรื่อง (Issue-specific Security Policy : ISSP) คือ การแสดงรายละเอียดการแนะแนวทางแก่สมาชิกทุกคนในองค์กร ในการใช้กระบวนการ เทคโนโลยี หรือระบบที่มีในองค์กร มี 3 คุณลักษณะ ดังนี้

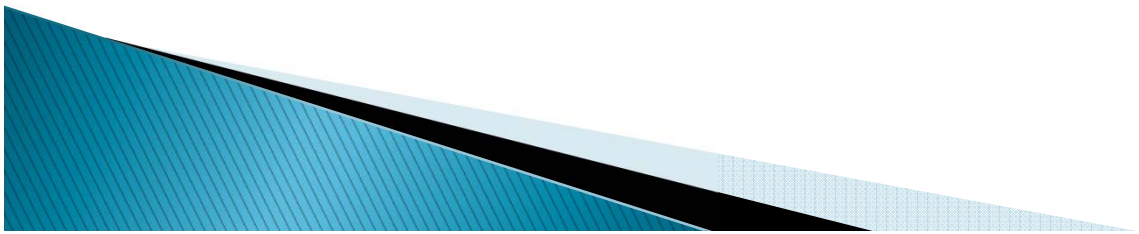
1. ระบุรายละเอียดเป็นเรื่อง ๆ จำแนกตามเทคโนโลยีแต่ละชนิด
2. ต้องมีการปรับปรุงข้อมูลในนโยบายตามการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศ
3. มีการอธิบายสถานะขององค์กรที่เป็นอยู่ในแต่ละเรื่อง



นโยบายความมั่นคงปลอดภัยของสารสนเทศเฉพาะเรื่อง

ISSP มีองค์ประกอบ ดังนี้

1. วัตถุประสงค์ (Statement of Purpose)
2. การใช้งานที่ได้รับอนุญาต (Authorized Uses)
3. การใช้งานที่ไม่ได้รับอนุญาต (Prohibited Uses)
4. การจัดการระบบ (Systems Management)
5. การละเมิดนโยบาย (Violations of Policy)
6. การทบทวนนโยบายและการแก้ไข (Policy Review and Modification)
7. ความรับผิดชอบ (Limitations of Liability)



นโยบายความมั่นคงปลอดภัยของสารสนเทศเฉพาะเรื่อง

ISSP มีแนวทางการจัดทำ ดังนี้

1. Individual Policy จัดทำเอกสารนโยบาย ISSP ของแต่ละเทคโนโลยีสารสนเทศแยกกัน ไม่รวมอยู่ด้วยกัน

ข้อดี

1. สามารถมอบหมายงานจัดทำนโยบายให้กับแผนกที่เกี่ยวข้องได้อย่างชัดเจน
2. นโยบายถูกเขียนโดยผู้เชี่ยวชาญของแต่ละแผนก

ข้อเสีย

1. ไม่ครอบคลุมส่วนอื่นเท่าที่จำเป็น
2. อาจทำให้การเผยแพร่ การบังคับใช้ และการทบทวนนโยบายทั้งหมดไม่มีประสิทธิภาพ

นโยบายความมั่นคงปลอดภัยของสารสนเทศเฉพาะเรื่อง

ISSP มีแนวทางการจัดทำ ดังนี้

2. Comprehensive Policy จัดทำเอกสารนโยบาย ISSP เพียงชุดเดียว

ข้อดี

1. ควบคุมเนื้อหาในเอกสารนโยบายให้ครบถ้วนได้โดยง่าย
2. กำหนดลำดับขั้นตอนในการจัดทำเป็นแบบแผนได้ดีกว่า Individual
3. กำหนดขั้นตอนเผยแพร่ บังคับใช้ และทบทวน ให้เป็นกระบวนการเดียว

ข้อเสีย

1. เป็นกลางมากเกินไป จนทำให้เกิดช่องโหว่
2. อาจถูกเขียนโดยผู้เชี่ยวชาญน้อยในประเด็นสำคัญ

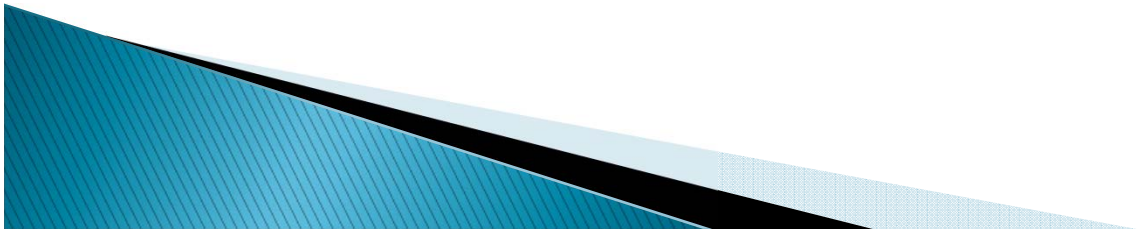
นโยบายความมั่นคงปลอดภัยของสารสนเทศเฉพาะเรื่อง

ISSP มีแนวทางการจัดทำ ดังนี้

3. Modular Policy จัดทำเอกสารนโยบาย ISSP โดยรวมทั้ง Individual and Comprehensive เข้าด้วยกัน

ข้อดี

1. รวมข้อดีทั้ง Individual and Comprehensive เข้าด้วยกัน
2. ควบคุมการจัดทำได้ง่าย และครอบคลุมทุกเรื่อง
3. มอบหมายงานให้กับแผนกที่เกี่ยวข้องได้อย่างชัดเจน
4. นโยบายถูกเขียนโดยผู้เชี่ยวชาญแต่ละแผนก

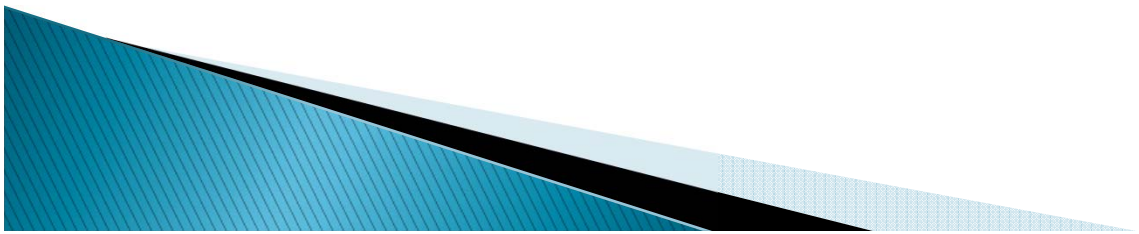


นโยบายความมั่นคงปลอดภัยของสารสนเทศเฉพาะระบบ

นโยบายความมั่นคงปลอดภัยเฉพาะระบบ (System-specific Security Policy : SysSP) คือการกำหนดมาตรฐานและวิธีการปฏิบัติ ที่จะนำไปใช้ในการกำหนดค่าคุณสมบัติหรือการบำรุงรักษาระบบ แต่ต้องไม่ขัดกับ ISSP and EISP

SysSP แบ่งออกเป็น 2 กลุ่ม คือ

1. แนวทางด้านบริหาร (Managerial Guidance)
2. ข้อกำหนดทางเทคนิค (Technical Specification)



ขั้นตอนในการจัดทำและนำนโยบายไปใช้งาน

Information Security Program

หมายถึง การดำเนินการ (Operations) ใด ๆ ที่ถูกจัดทำขึ้นเพื่อความมั่นคงปลอดภัยของสารสนเทศ ซึ่งการดำเนินงานนั้นถูกบริหารจัดการแยกเป็นพิเศษ (Separate Entity)

หมายถึง โครงสร้างและความพยายามที่จะยับยั้งความเสี่ยงที่มีต่อสารสนเทศขององค์กร ซึ่งมีปัจจัย ที่ทำให้ส่วนงานความมั่นคงปลอดภัยของสารสนเทศในแต่ละองค์กรแตกต่างกัน ได้แก่

1. วัฒนธรรมขององค์กร (Organization Culture)
2. ขนาดขององค์กร (Organization Size)
3. งบประมาณที่ได้รับ (Information Security Budget)

Information Security Program

ภาระงานของส่วนงานความมั่นคงปลอดภัยของสารสนเทศ เช่น

1. การประเมินความเสี่ยง (Risk Assessment)
2. การจัดการความเสี่ยง (Risk Management)
3. การทดสอบระบบ (System Testing)
4. จัดทำนโยบาย (Policy)
5. การประเมินทางกฎหมาย (Legal Assessment)
6. การรับมือกับเหตุการณ์ไม่คาดคิด (Incident Response)
7. การวางแผน (Planning)
8. การวัดผล (Measurement)

Information Security Program

ภาระงานของส่วนงานความมั่นคงปลอดภัยของสารสนเทศ เช่น

9. การปฏิบัติตามกฎหมาย (Compliance)

10. การพิสูจน์ตัวตน (Authentication)

11. การดูแลความมั่นคงปลอดภัยของระบบ (System Security Adm.)

12. การฝึกอบรม (Training)

13.การดูแลความมั่นคงปลอดภัยของเครือข่าย (Network Security Adm.)

14. การประเมินช่องโหว่ (Vulnerability Assessment)

ซึ่งส่วนงานจะรับผิดชอบทั้งหมดหรือไม่ ขึ้นอยู่กับขนาดขององค์กร และการจัดสร้างองค์กรของส่วนงานด้วย

Questions and Answers

MS1 Thanin Muangpool

Thank you