
ความมั่นคงปลอดภัยของสารสนเทศ
INFORMATION SECURITY
Company LOGO

ความมั่นคงปลอดภัยของสารสนเทศ

- ความมั่นคงปลอดภัยของสารสนเทศคืออะไร
- แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ
- แนวคิดของความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน NSTISSC
- องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย
- แนวทางในการดำเนินงานความมั่นคงปลอดภัยของสารสนเทศ
- วงจรการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ
- บทบาทของบุคลากรสารสนเทศในด้านความมั่นคงปลอดภัย

ความมั่นคงปลอดภัยของสารสนเทศคืออะไร

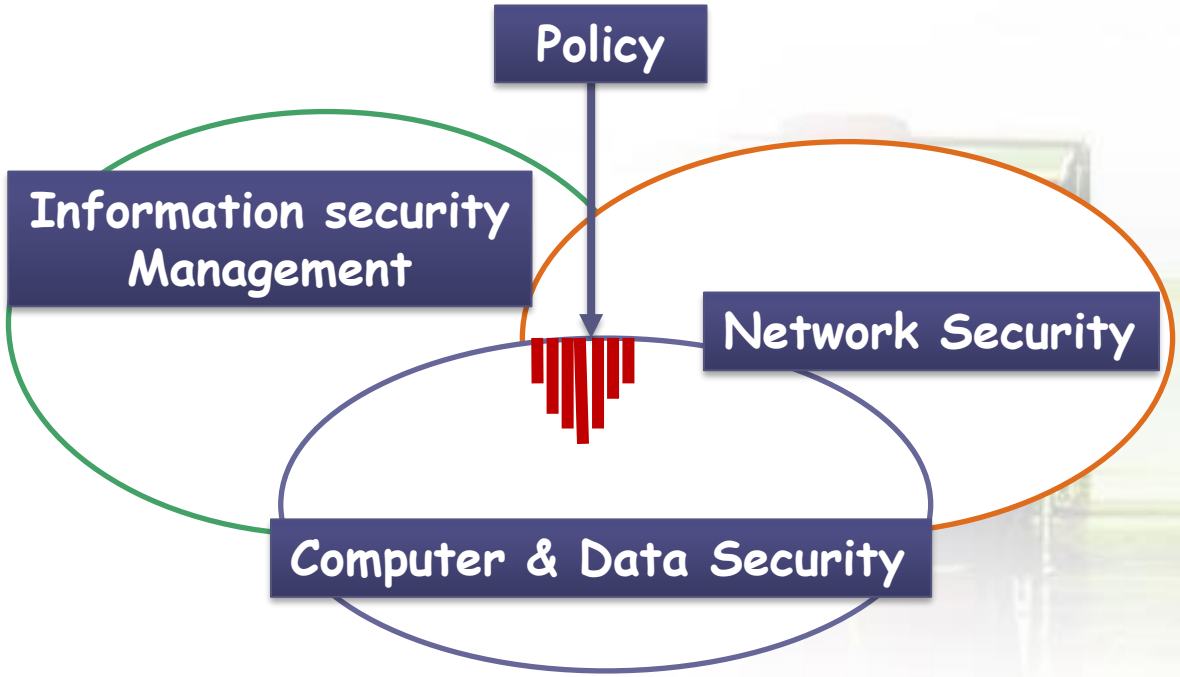
- **ความมั่นคงปลอดภัย (Security) คือ สถานะที่มีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ**
- เช่น ความมั่นคงปลอดภัยของประเทศ ย่อมเกิดขึ้นโดยมีระบบป้องกันหลายระดับ เพื่อปกป้องผู้นำประเทศ ทรัพย์สิน ทรัพยากร และประชาชนของประเทศ

ความมั่นคงปลอดภัยขององค์กร

- ความมั่นคงปลอดภัยทางกายภาย Physical Security
- ความมั่นคงปลอดภัยส่วนบุคคล Personal Security
- ความมั่นคงปลอดภัยในการปฏิบัติงาน Operations Security
- ความมั่นคงปลอดภัยในการติดต่อสื่อสาร Communication Security
- ความมั่นคงปลอดภัยของเครือข่าย Network Security
- ความมั่นคงปลอดภัยของสารสนเทศ Information Security

Information Security

- ความมั่นคงปลอดภัยของสารสนเทศ คือ การป้องกันสารสนเทศและองค์ประกอบอื่นที่เกี่ยวข้อง



Information Security

- การรักษาความปลอดภัยทางข้อมูล Information Security คือ ผลที่เกิดขึ้นจากการใช้ระบบของนโยบายและ/ หรือ ระเบียบปฏิบัติที่ใช้ในการพิสูจน์ทราบ ควบคุม และป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการป้องกัน) โดยไม่ได้รับอนุญาต

- นิยามโดย ThaiCERT (ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

- **กลุ่มอุตสาหกรรมความมั่นคงปลอดภัยของคอมพิวเตอร์ ได้กำหนดแนวคิดหลักของความมั่นคงปลอดภัยของคอมพิวเตอร์ขึ้น**

ประกอบด้วย C.I.A Triangle

1. **ความลับ Confidentiality**
2. **ความสมบูรณ์ Integrity**
3. **ความพร้อมใช้ Availability**
4. ความถูกต้องแม่นยำ Accuracy
5. เป็นของแท้ Authenticity
6. ความเป็นส่วนตัว Privacy

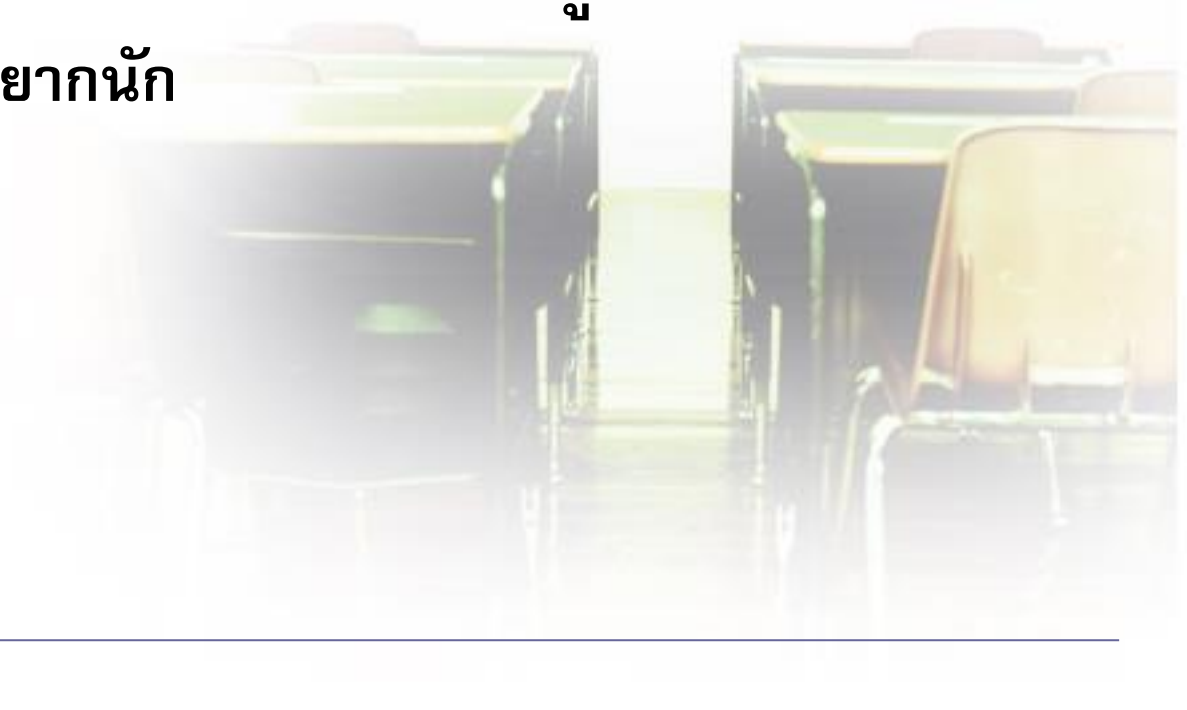
ความลับ Confidentiality

- **เป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้**

- **องค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ เช่น**
  - การจัดประเภทของสารสนเทศ
  - การรักษาความปลอดภัยในกับแหล่งจัดเก็บข้อมูล
  - กำหนดนโยบายรักษาความมั่นคงปลอดภัยและนำไปใช้
  - ให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและผู้ใช้

ความลับ Confidentiality

- ภัยคุกคามที่เพิ่มมากขึ้นในปัจจุบัน มีสาเหตุมาจากความก้าวหน้าทางเทคโนโลยี ประกอบกับความต้องการความสะดวกสบายในการสั่งซื้อสินค้าของลูกค้า โดยการยอมให้สารสนเทศส่วนบุคคลแก่ website เพื่อสิทธิ์สนการทำธุรกรรมต่าง ๆ โดยลืมไปว่าเว็บไซต์เป็นแหล่งข้อมูลที่สามารถขโมยสารสนเทศไปได้ไม่ยากนัก



ความสมบูรณ์ Integrity

- ความสมบูรณ์ คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอม สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องครบถ้วน

- สารสนเทศจะขาดความสมบูรณ์ ก็ต่อเมื่อสารสนเทศนั้นถูกนำไปเปลี่ยนแปลง ปลอมปนด้วยสารสนเทศอื่น ถูกทำให้เสียหาย ถูกทำลาย หรือถูกกระทำในรูปแบบอื่น ๆ เพื่อขัดขวางการพิสูจน์การเป็นสารสนเทศจริง

ความพร้อมใช้ Availability

- ความพร้อมใช้ หมายถึง สารสนเทศจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้หรือระบบอื่นที่ได้รับอนุญาตเท่านั้น

- หากเป็นผู้ใช้หรือระบบที่ไม่ได้รับอนุญาต การเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลวในที่สุด

ความถูกต้องแม่นยำ Accuracy

- ความถูกต้องแม่นยำ หมายถึง สารสนเทศต้องไม่มีความผิดพลาด และต้องมีค่าตรงกับความคาดหวังของผู้ใช้เสมอ

- เมื่อใดก็ตามที่สารสนเทศมีค่าผิดเพี้ยนไปจากความคาดหวังของผู้ใช้ ไม่ว่าจะเกิดจากการแก้ไขด้วยความตั้งใจหรือไม่ก็ตาม เมื่อนั้นจะถือว่าสารสนเทศ ไม่มีความถูกต้องแม่นยำ

ความเป็นของแท้ Authenticity

- สารสนเทศที่เป็นของแท้ คือ สารสนเทศที่ถูกจัดทำขึ้นจากแหล่งที่ถูกต้อง ไม่ถูกทำซ้ำโดยแหล่งอื่นที่ไม่ได้รับอนุญาต หรือแหล่งที่ไม่คุ้นเคยและไม่เคยทราบมาก่อน

ความเป็นส่วนตัว Privacy

- ความเป็นส่วนตัว คือ สารสนเทศที่ถูกรวบรวม เรียกใช้ และจัดเก็บโดยองค์กร จะต้องถูกใช้ในวัตถุประสงค์ที่ผู้เป็นเข้าของสารสนเทศรับทราบ ณ ขณะที่มีการรวบรวมสารสนเทศนั้น

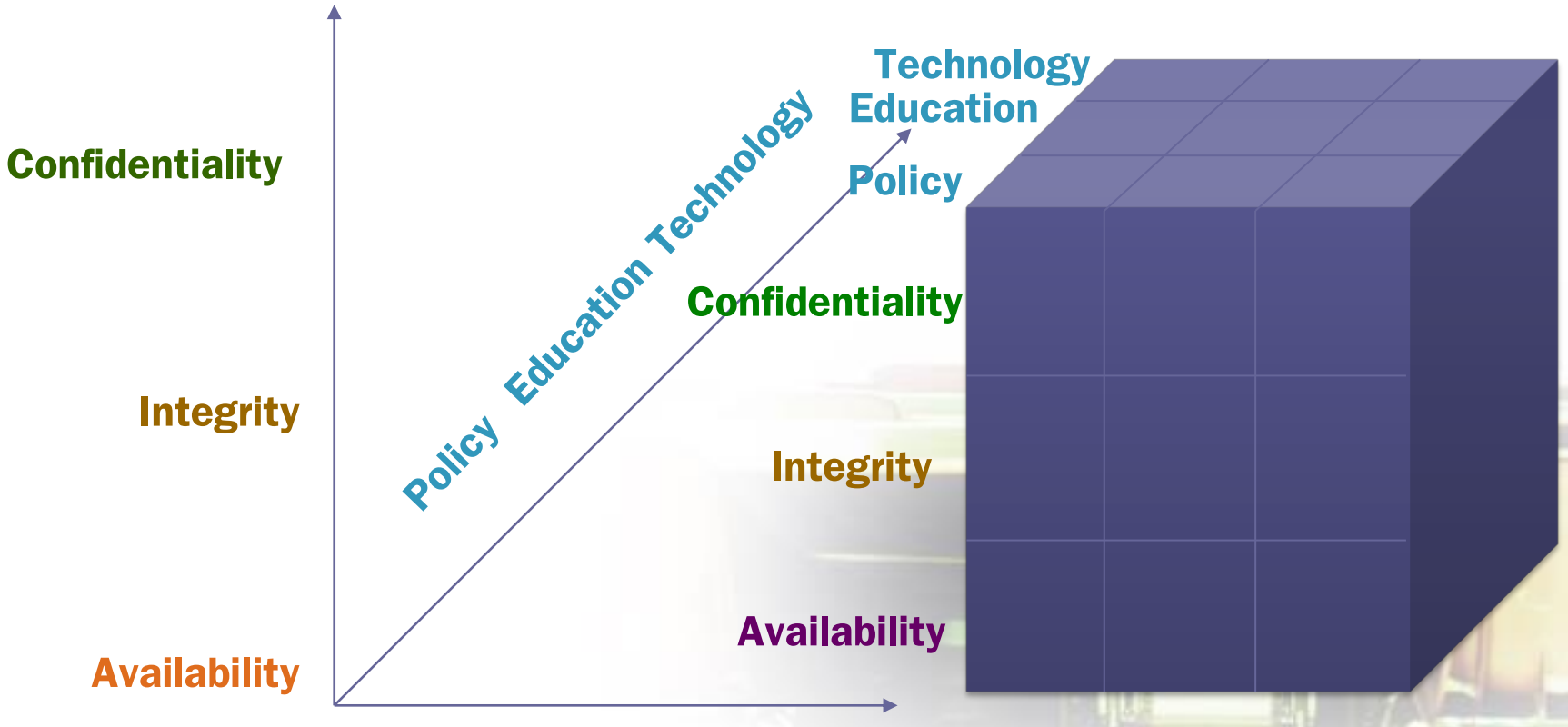
- มิฉะนั้นจะถือว่าเป็นการละเมิดสิทธิส่วนบุคคลด้านสารสนเทศ

แนวคิดของความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน NSTISSC

- **NSTISSC （Nation Security Telecommunications and Information Systems Security**

- คือ คณะกรรมการด้านความมั่นคงโทรคมนาคมและระบบสารสนเทศแห่งชาติของต่างประเทศที่ได้รับการยอมรับแห่งหนึ่งได้กำหนดแนวคิดความมั่นคงปลอดภัยขึ้นมา ต่อมาได้กลายเป็นมาตรฐานการประเมินความมั่นคงของระบบสารสนเทศ

แนวคิดของความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน NSTISSC



แสดงแนวคิดความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน NSTISSC

แนวคิดของความมั่นคงปลอดภัยของสารสนเทศตามมาตรฐาน NSTISSC

- สิ่งสำคัญในการดำเนินงานความมั่นคงปลอดภัยของสารสนเทศนั้น นอกจากจะมีความคิดหลักในด้านต่าง ๆ แล้ว ยังรวมถึงการกำหนดนโยบายการปฏิบัติงาน การให้การศึกษา และเทคโนโลยีที่จะนำมาใช้เป็นกลไกควบคุมและป้องกัน ที่ต้องเกี่ยวข้องกับการจัดการความมั่นคงปลอดภัยของสารสนเทศด้วย

องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย

1. **Software** ย่อมต้องอยู่ภายใต้เงื่อนไขของการบริหารโครงการ ภายใต้เวลา ต้นทุน และกำลังคนที่จำกัด ซึ่งมักจะทำภายหลังจากการพัฒนาซอฟต์แวร์เสร็จแล้ว

องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย

- **Hardware** จะใช้นโยบายเดียวกับสินทรัพย์ที่จับต้องได้ขององค์กร คือการป้องกันจากการลักขโมยหรือภัยอันตรายต่าง ๆ รวมถึงการจัดสถานที่ที่ปลอดภัยให้กับอุปกรณ์หรือฮาร์ดแวร์

องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย

- **Data ข้อมูล/สารสนเทศ** เป็นทรัพยากรที่มีค่าขององค์กร การป้องกันที่แน่นหนาก็มีความจำเป็นสำหรับข้อมูลที่เป็นความลับ ซึ่งต้องอาศัยนโยบายความปลอดภัยและกลไกป้องกันที่ดีควบคู่กัน

องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย

- **People บุคลากร** คือภัยคุกคามต่อสารสนเทศที่ถูกมองข้ามมากที่สุด โดยเฉพาะบุคลากรที่ไม่มีจรรยาบรรณในอาชีพ ก็เป็นจุดอ่อนต่อการโจมตีได้ จึงได้มีการศึกษากันอย่างจริงจัง เรียกว่า **Social Engineering** ซึ่งเป็นการป้องการการหลอกหลวงบุคลากรเพื่อเปิดเผยข้อมูลบางอย่างเข้าสู่ระบบได้

องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย

- **Procedure** ขั้นตอนการทำงาน เป็นอีกหนึ่งองค์ประกอบที่ถูกมองข้าม หากมิจฉาชีพทราบขั้นตอนการทำงาน ก็จะสามารถค้นหาจุดอ่อนเพื่อนกระทำการอันก่อนให้เกิดความเสียหายต่อองค์กรและลูกค้าขององค์กรได้

องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย

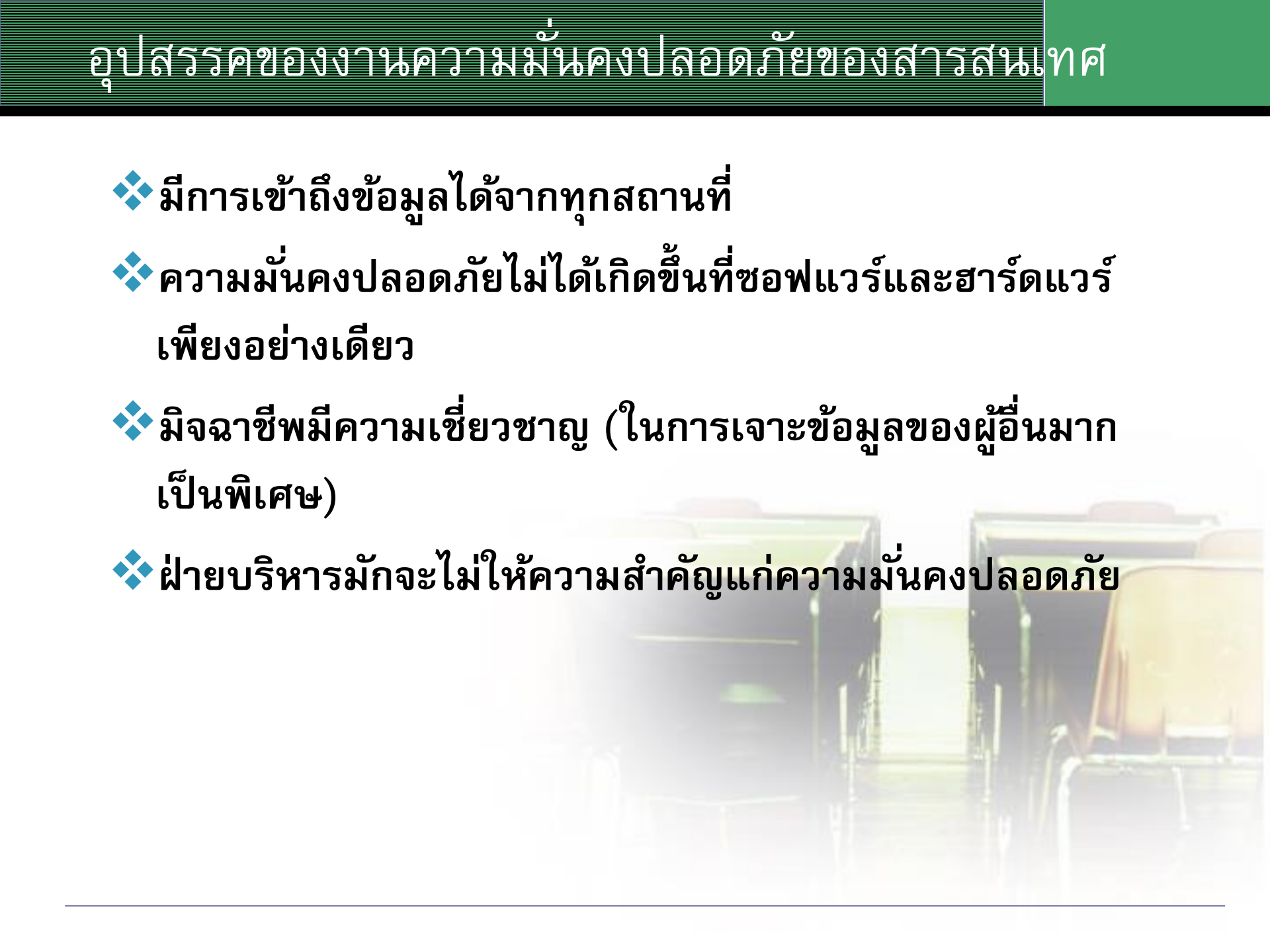
- **Network** เครือข่ายคอมพิวเตอร์ การเชื่อมต่อระหว่างคอมพิวเตอร์และระหว่างเครือข่ายคอมพิวเตอร์ ทำให้เกิดอาชญากรรมและภัยคุกคามคอมพิวเตอร์ โดยเฉพาะการเชื่อมต่อระบบสารสนเทศเข้ากับเครือข่ายอินเตอร์เน็ต

อุปสรรคของงานความมั่นคงปลอดภัยของสารสนเทศ

- ความมั่นคงปลอดภัย คือ ความไม่สะดวก เนื่องจากต้องเสียเวลาในการป้อน password และกระบวนการอื่น ๆ ในการพิสูจน์ตัวผู้ใช้
- มีความซับซ้อนบางอย่างในคอมพิวเตอร์ที่ผู้ใช้ทั่วไปไม่ทราบ เช่น Registry , Port, Service ที่เหล่านี้จะทราบในแวดวงของ Programmer หรือผู้ดูแลระบบ
- ผู้ใช้คอมไม่ระแวดระวัง
- การพัฒนาซอฟต์แวร์ไม่คำนึงถึงความปลอดภัยภายหลัง
- แนวโน้มเทคโนโลยีสารสนเทศคือการแบ่งปัน ไม่ใช่ การป้องกัน

อุปสรรคของงานความมั่นคงปลอดภัยของสารสนเทศ

- มีการเข้าถึงข้อมูลได้จากทุกสถานที่
- ความมั่นคงปลอดภัยไม่ได้เกิดขึ้นที่ซอฟแวร์และฮาร์ดแวร์เพียงอย่างเดียว
- มิจฉาชีพมีความเชี่ยวชาญ (ในการเจาะข้อมูลของผู้อื่นมากเป็นพิเศษ)
- ฝ่ายบริหารมักจะไม่ให้ความสำคัญแก่ความมั่นคงปลอดภัย



แนวทางในการดำเนินงานความมั่นคงปลอดภัยของสารสนเทศ

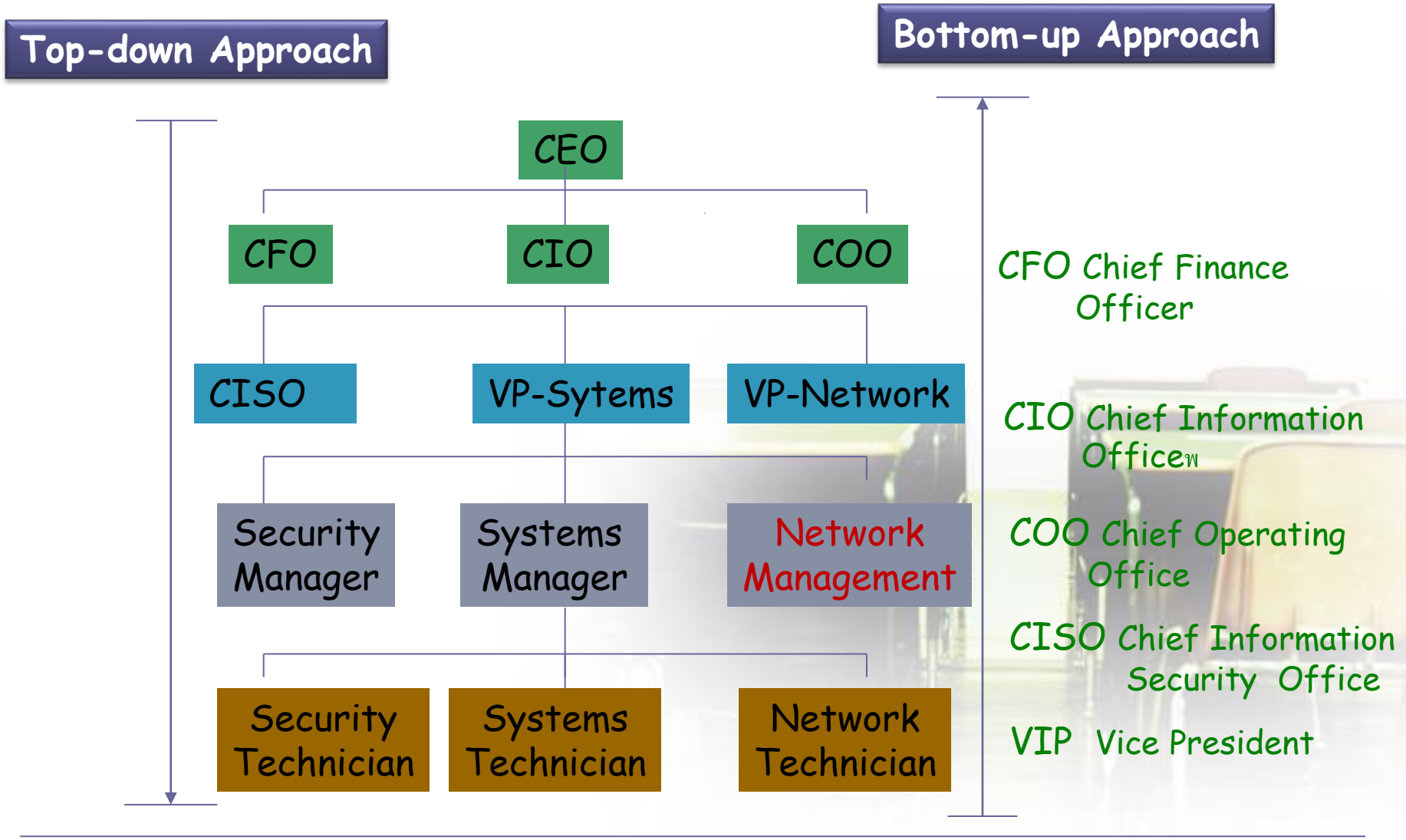
- **Boottom –Up Approach** เป็นแนวทางที่ผู้ดูแลระบบหรือเจ้าหน้าที่ที่รับผิดชอบด้านความมั่นคงปลอดภัยโดยตรง เป็นผู้ริเริ่มหรือกำหนดมาตรการรักษาความปลอดภัย ขึ้นมาระหว่างการพัฒนาระบบ
- **ข้อดี** คือ เจ้าหน้าที่จะสามารถดูแลงานด้วยตนเองในทุก ๆ วัน และใช้ความรู้ความสามารถ ความเชี่ยวชาญที่มีการปรับปรุงกลไกควบคุมความปลอดภัยให้มีประสิทธิภาพอย่างเต็มที่
- **ข้อเสีย** แนวทางนี้ โดยทั่วไปมักจะทำให้การดำเนินงานความมั่นคงปลอดภัยของสารสนเทศไม่ประสบผลสำเร็จ เนื่องจากขาดปัจจัยความสำเร็จ เช่น ขาดการสนับสนุนจากผู้เกี่ยวข้องหรือขาดอำนาจหน้าที่ในการสั่งการ

แนวทางในการดำเนินงานความมั่นคงปลอดภัยของสารสนเทศ

- **Top-down Approach** การดำเนินงานความมั่นคงปลอดภัยจะเริ่มต้นโดยผู้บริหารหรือผู้มีอำนาจหน้าที่โดยตรง ซึ่งสามารถบังคับใช้นโยบาย บุคลากรที่รับผิดชอบ

- **ข้อดี** ขั้นตอนกระบวนการมั่นคงได้อย่างเต็มที่ เนื่องจากได้รับการสนับสนุนจากผู้ที่เกี่ยวข้องเป็นอย่างดี มีการวางแผนกำหนดเป้าหมาย และกระบวนการทำงานอย่างชัดเจนและเป็นทางการ

แนวทางในการดำเนินงานความมั่นคงปลอดภัยของสารสนเทศ



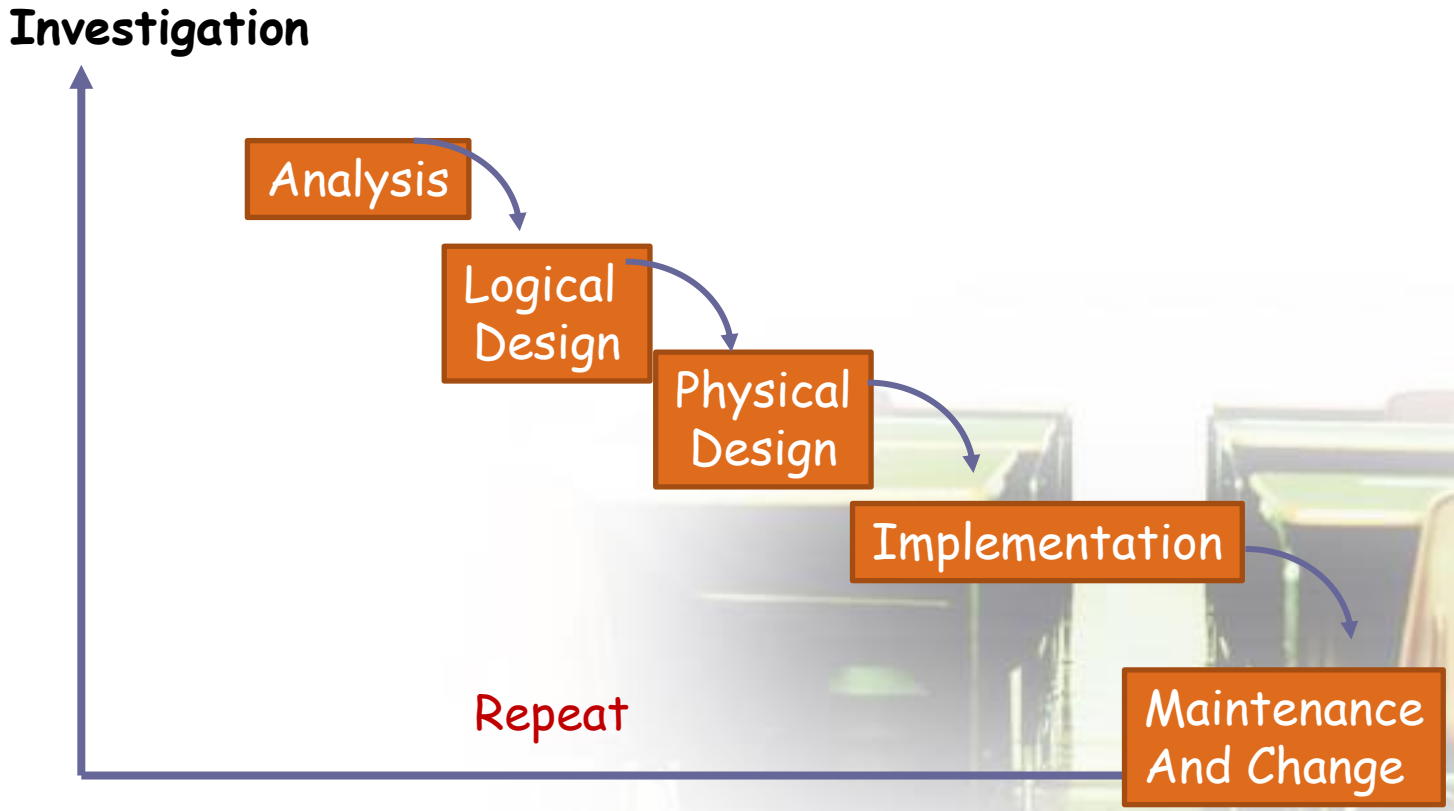
วงจรการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ

- วงจรการพัฒนาระบบ System Development life Cycle: SDLC โดยแต่ละ Phase ของ SDLC สามารถนำมาปรับใช้กับการดำเนินโครงการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศได้ เรียกว่า Security Systems Development Life Cycle : SecSDLC

- บางองค์กร สามารถใช้วิธีการจัดการความเสี่ยง Risk Management เป็นกระบวนการหลักในการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศได้

วงจรการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ

SDLC เมื่อถูกนำไปปรับใช้ในองค์กร จะถูกแบ่ง
เฟส phase ในจำนวนที่แตกต่างกัน



เมื่อนำมาปรับใช้กับการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ

วงจรการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ

- **การสำรวจ Investigation** เริ่มจากได้รับคำสั่งจากผู้บริการระดับสูง ให้ดำเนินการพัฒนาระบบความมั่นคงปลอดภัย โดยมีการกำหนดเป้าหมาย กระบวนการ ผลลัพธ์ที่ต้องการ บุคลากร งบประมาณ และระยะเวลา ยังมีการกำหนดนโยบายความมั่นคงปลอดภัยในระดับองค์กรมาพร้อมกันด้วย
- ทีมงานที่รับผิดชอบจะนำรายละเอียดทำการสำรวจ เพื่อนำมาวิเคราะห์ปัญหา กำหนดขอบเขต เป้าหมายและวัตถุประสงค์ของโครงการ

วงจรการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ

- การวิเคราะห์ Analysis เป็นเฟสที่ทีมงานจะได้นำเอกสารมาทำการศึกษาเพิ่มเติม ศึกษาถึงภัยคุกคาม และวิธีป้องกัน รวมถึงกฎหมายสิทธิส่วนบุคคล การจัดการความเสี่ยง (ระบุความเสี่ยง)
- ประเมินหาความเสี่ยงที่มีผลกระทบในระดับร้ายแรง พร้อมกันเตรียมป้องกันไม่ให้เกิดความเสี่ยงต่าง ๆ ได้อีก

วงจรการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ

- การออกแบบระดับตรรกะ **Logical Design** เป็นเฟสที่ต้องจัดทำโครงร่างของระบบความมั่นคงปลอดภัยของสารสนเทศ ตรวจสอบและจัดทำนโยบายหลักที่จะนำไปใช้

วงจรการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ

- การออกแบบระดับกายภาพ **Physical Design** เป็นเฟสการกำหนดเทคโนโลยีสารสนเทศที่จะนำมาสนับสนุนโครงร่างระบบความมั่นคงปลอดภัยที่ได้ออกแบบไว้ในเฟสที่ผ่านมา มีการประเมินเทคโนโลยี พร้อมกับสร้างทางเลือกของเทคโนโลยีที่จะนำมาใช้

วงจรการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ

- การพัฒนา **Implementation** ดำเนินงานพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศที่ได้ออกแบบไว้ให้เกิดขึ้นจริง และทำการทดสอบ จนกว่าไม่พบข้อผิดพลาด

วงจรการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ

- การบำรุงรักษาและเปลี่ยนแปลง **Maintenance and Change** การติดตาม ทดสอบแก้ไข และซ่อมบำรุงอยู่ตลอดเวลา ควรมีการอัพเดทภัยคุมคาม รายละเอียดให้ทันสมัยอยู่อย่างสม่ำเสมอ

การเปรียบเทียบกิจกรรมใน SDLC /SecSDLC

เฟส	กิจกรรมใน SDLCธรรมดา	กิจกรรมในSecSDLC
1 Investigation	•กำหนดเป้าหมายและขอบเขตโครงการ •ประมาณต้นทุน •ประเมินทรัพยากร •ศึกษาความเป็นไปได้	ผู้บริหารกำหนดกระบวนการดำเนินโครงการ เป้าหมาย และเอกสารแสดงนโยบายความมั่นคงที่มีอยู่

การเปรียบเทียบกิจกรรมใน SDLC /SecSDLC

เฟส	กิจกรรมใน SDLCธรรมดา	กิจกรรมในSecSDLC
2 Analysis	•ศึกษาระบบเดิมตามเอกสารที่ได้รับในเฟสแรก •กำหนดความต้องการของระบบ •ศึกษาการประสานงานระบบเก่ากับระบบใหม่ •จัดทำเอกสาร และปรับปรุงศึกษาความเป็นไปได้	•วิเคราะห์นโยบายความมั่นคงปลอดภัยเดิม •วิเคราะห์ภัยคุกคาม •พิจารณาประเด็นกฎหมาย •วิเคราะห์ความเสี่ยง

การเปรียบเทียบกิจกรรมใน SDLC /SecSDLC

เฟส	กิจกรรมใน SDLCธรรมดา	กิจกรรมในSecSDLC
3 **Logical Design**	•ประเมินความจำเป็นทางธุรกิจ •เลือกข้อมูลสนับสนุนและโครงสร้างของระบบ •สร้างทางเลือกของระบบใหม่ •จัดทำเอกสารและปรับปรุงแก้ไข	•จัดทำโครงร่างระบบความมั่นคงปลอดภัย •วางแผนรับมือเหตุการณ์ไม่คาดคิด •วางแผนฟื้นฟูความเสียหาย

การเปรียบเทียบกิจกรรมใน SDLC /SecSDLC

เฟส	กิจกรรมใน SDLCธรรมดา	กิจกรรมในSecSDLC
4 **Physical Design**	•เลือกเทคโนโลยีที่จะนำมาสนับสนุนระบบ •เลือกทางเลือกของระบบ •ตัดสินใจว่าจะซื้อหรือจะพัฒนาระบบเอง •จัดทำเอกสาร และปรับปรุงแก้ไข รายงานการศึกษาความเป็นไปได้	•เลือกเทคโนโลยีที่จะนำสนับสนุนโครงการ •กำหนดนิยาม •กำหนดเงื่อนไขในการคัดเลือกเทคโนโลยีความมั่นคงปลอดภัย •ทบทวนและพิจารณาอนุมัติโครงการ

การเปรียบเทียบกิจกรรมใน SDLC /SecSDLC

เฟส	กิจกรรมใน SDLCธรรมดา	กิจกรรมใน SecSDLC
5 Implementation	•พัฒนาหรือระบบใหม่ •สั่งซื้อ componentของระบบใหม่ •จัดทำเอกสารของระบบ •ฝึกอบรมผู้ใช้ •นำเสนอระบบต่อผู้ใช้ •ทดสอบระบบ	•ซื้อหรือพัฒนาระบบ •นำเสนอต่อผู้บริหารระดับสูง

การเปรียบเทียบกิจกรรมใน SDLC /SecSDLC

เฟส	กิจกรรมใน SDLCธรรมดา	กิจกรรมในSecSDLC
6 Maintenance and Change	•สนับสนุนการใช้งานระบบ •ทดสอบระบบอยู่เป็นระยะ •อัดเกรดและซ่อมบำรุงระบบตามความจำเป็น	ติดตาม ทำสอบ แก้ไข อัพเดท และซ่อมบำรุงระบบทันทีที่พบว่ามีภัยคุกคาม

บทบาทของบุคลากรสารสนเทศในด้านความมั่นคงปลอดภัย

1.ผู้บริการระดับสูง Senior Manager

1.1. ผู้บริหารสารสนเทศระดับสูง chief Information

Officer : CIO มีหน้าที่ให้คำแนะนำและแสดงความคิดเห็นแก่ ผู้บริหารระดับสูง

1.2. ผู้บริหารความมั่นคงปลอดภัยของสารสนเทศระดับสูง

Chief Information Security Officer : CISO ทำหน้าที่ในการประเมิน จัดการ และพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศในองค์กรโดยเฉพาะ

2.ทีมงานดำเนินโครงการความมั่นคงปลอดภัยของสารสนเทศ

Information Securtiy Project Team

ทีมงานดำเนินโครงการ ควรเป็นผู้ที่มีความรู้ ความสามารถในด้านเทคโนโลยีอย่างลึกซึ้ง และควรจะมีความรู้ในด้านอื่นๆ ที่เกี่ยวข้องควบคู่ไปด้วย

ทีมงานดำเนินโครงการประกอบไปด้วย

- ผู้สนับสนุน Champion
- หัวหน้าทีม Team Leader
- นักพัฒนานโยบายความมั่นคงปลอดภัย Security Policy Development
- ผู้ชำนาญการประเมินความเสี่ยง Risk Assessment Specialist
- ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของสารสนเทศ Security Professional
- ผู้ดูแลระบบ System Administrator
- ผู้ใช้ระบบ End User

บทบาทของบุคลากรสารสนเทศในด้านความมั่นคงปลอดภัย

3.การเป็นเจ้าของข้อมูล Data Ownership ประกอบด้วย

3.1 เจ้าของข้อมูล Data Owners ผู้มีสิทธิในการใช้ข้อมูล และมีหน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลด้วย

3.2 ผู้ดูแลข้อมูล Data Cusodians เป็นผู้ที่ต้องทำงานร่วมกับ Data Owners โดยตรง ทำหน้าที่จัดเก็บและบำรุงรักษาข้อมูล

3.3 ผู้ใช้ข้อมูล Data Users เป็นผู้ที่ทำงานกับข้อมูล โดยตรง

สรุป

- ความมั่นคงปลอดภัยของสารสนเทศ **Information Security** คือการป้องกันสารสนเทศและองค์ประกอบอื่น ๆ ที่เกี่ยวข้อง

สรุป

- แนวคิด C.I.A Triangle ประกอบไปด้วย
  - ความลับ Confidentiality
  - ความสมบูรณ์ Integrity
  - ความพร้อมใช้ Availability

และยังกำหนดเพิ่มอีก คือ

- ความถูกต้องแม่นยำAccuracy
- ความเป็นของแท้ Authenticity
- และความเป็นส่วนตัว Privacy

สรุป

แนวทางในการดำเนินงานความมั่นคงปลอดภัยของสารสนเทศ

มี 2 ลักษณะ คือ

1. **Bottom-Up Approach** คือผู้ดูแลระบบหรือทีมงานเป็นผู้ริเริ่มโครงการ

2. **Top-down Approach** คือผู้บริหารระดับสูงเป็นผู้ริเริ่มและกำหนดโครงการ

สรุป

วงจรการพัฒนาระบบความมั่นคงปลอดภัยของสารสนเทศ

มี 6 เฟส คือ

- การสำรวจ Investigation
- การวิเคราะห์ Analysis
- การออกแบบระดับตรรกะ Logical Design
- การออกแบบและพัฒนากายภาพ Physical Design
- การพัฒนา Implementation
- การบำรุงรักษาและเปลี่ยนแปลง Maintenance and Change

สรุป

บุคคลที่เกี่ยวข้องกับระบบความมั่นคงปลอดภัยของสารสนเทศ

- ผู้บริหารสารสนเทศระดับสูง
- ผู้บริหารความมั่นคงปลอดภัยของสารสนเทศระดับสูง
- ผู้บริหารโครงการ หรือหัวหน้าทีม
- เจ้าหน้าที่เทคนิคด้านความมั่นคงปลอดภัยของสารสนเทศ เป็นต้น