



# เทคนิคการออกแบบ มาตรการความปลอดภัย ของข้อมูล

## Data Protection System

หลักสูตรนี้ออกแบบมาสำหรับเจ้าหน้าที่ทุกหน่วยงานที่เกี่ยวข้องกับการจัดเก็บ ใช้ เปิดเผยข้อมูล และสร้างความตระหนักถึงความปลอดภัยของข้อมูล ที่หลายๆท่าน อาจไม่ได้วางระบบป้องกัน การคุกคามอย่างที่ถ้วน หากมาตรการการป้องกันไม่ดีพอ จะส่งผลถึงการรั่วไหลของข้อมูล

- ✓ เรียนรู้เทคนิคการจัดเก็บข้อมูลอย่างถูกต้องและปลอดภัย
- ✓ แนวทางการวางมาตรการความปลอดภัยแก่ข้อมูลที่มีมาตรฐานระดับสากล ISO 27701
- ✓ สิ่งสำคัญที่เจ้าหน้าที่ดูแลข้อมูลต้องระวัง “ข้อมูลรั่วไหล”
- ✓ Workshop : การออกแบบระบบ Data Flow ที่มีประสิทธิภาพและใช้ได้จริง!



### กำหนดการสัมมนา

วันพฤหัสบดีที่ 16 พฤษภาคม 2567

(เวลา 09.00 - 16.00) ณ ห้องสัมมนา

โรงแรมอินเตอร์คอนติเนนตัล กรุงเทพฯ  
(ฝั่งตึกฮอลิเดย์ อินน์)

รถไฟฟ้า BTS สถานีชิดลม ทางออกที่ 6

### อัตราค่าสัมมนา

สมาชิก (Tax, HR)

5,000 + VAT 350 = 5,350 บาท

บุคคลทั่วไป

5,700 + VAT 399 = 6,099 บาท

(รวมเอกสาร อาหารว่าง ชา กาแฟ อาหารกลางวัน)

## หัวข้อสัมมนา

1. หน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)
  - การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
  - การรักษาความมั่นคงปลอดภัยทางสารสนเทศ (Computer or Information Security)
  - การรักษาคุณภาพของข้อมูลหรือคุณภาพของสารสนเทศ (Data Quality)
2. ภัยคุกคามความมั่นคงปลอดภัยของข้อมูลหรือการละเมิดข้อมูล (Personal Data breach)
3. มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม (Appropriate measure)
  - ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม  
เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ.2563
  - ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล  
เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565
4. ปัจจัยเกี่ยวข้องกับความเสี่ยง (Risk) ของผลกระทบหรือความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล
5. มาตรการทางองค์กรหรือมาตรการด้านการบริหารจัดการ (Administrative or organization measure)
6. มาตรการทางเทคนิค (Technical measure)
7. การบริหารจัดการและการรักษาความปลอดภัยทางด้านระบบระบบไอที  
ให้สอดคล้องตามกฎหมายและมาตรฐาน ISO 27701
  - ขั้นตอนการบริหารจัดการข้อมูลส่วนบุคคล
  - การกำกับดูแลและควบคุมการใช้งานข้อมูลส่วนบุคคลขององค์กร
  - การจัดทำเอกสารสำหรับควบคุมการใช้ข้อมูลส่วนบุคคล
  - ขั้นตอนการบริหารจัดการความเสี่ยงและช่องโหว่ของระบบไอที  
ที่ส่งผลต่อความปลอดภัยของข้อมูลส่วนบุคคล
  - การกำหนดนโยบายทางด้านไอที (IT Policy) และการบังคับใช้
  - การวางระบบป้องกันการขโมยข้อมูล(Hack)หรือนำข้อมูลไปใช้โดยมิชอบ
  - การปฏิบัติเมื่อข้อมูลรั่วไหล (Data Leak) และวิธีการรับมือที่เหมาะสม
  - มาตรฐานการป้องกันความปลอดภัยของข้อมูลทางเทคนิคที่เกี่ยวข้อง
8. การแจ้งเหตุละเมิดข้อมูลส่วนบุคคล (Personal data breach notification)
  - เหตุผลของการแจ้งการละเมิดข้อมูลส่วนบุคคล
  - ผู้มีหน้าที่แจ้งและผู้รับแจ้ง
  - เงื่อนไขและข้อยกเว้นของการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล
  - เนื้อหาและรายละเอียดที่ต้องแจ้ง
9. Workshop : การออกแบบระบบ Data Flow จาก Case Study ที่ต้องระวัง
10. ถาม-ตอบประเด็นปัญหา และแลกเปลี่ยนความคิดเห็น

### วิทยากร

## อาจารย์กชณัช คงมีสุข

- ที่ปรึกษาด้านคณะกรรมการบริหาร เครือข่ายธุรกิจชั้นนำในประเทศไทย
- “นักจัดการคุ้มครองข้อมูลส่วนบุคคล” คุณวุฒิวิชาชีพแห่งชาติ สาขาความมั่นคงปลอดภัยทางดิจิทัล และส่วนบุคคล (TPQI)