หลักสูตร
การบริหารข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)
(Personal Data Management for PDPA)

❍ หลักการและเหตุผล

ปัจจุบันองค์กรมีการเก็บ ใช้ และเปิดเผยข้อมูลส่วนบุคคลในหลายกระบวนการ เช่น งานทรัพยากรบุคคล งานขาย การตลาด งานบริการลูกค้า งานจัดซื้อ งาน IT และงานบริหารจัดการภายใน ซึ่งหากไม่มีการควบคุมอย่างเหมาะสม อาจก่อให้เกิดความเสี่ยงทั้งด้านกฎหมาย ชื่อเสียง และความเชื่อมั่นจากลูกค้า พนักงาน และคู่ค้า

กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA: Personal Data Protection Act) จึงถูกประกาศใช้เพื่อกำหนดแนวทางที่ชัดเจนในการบริหารข้อมูลส่วนบุคคลอย่างถูกต้อง โปร่งใส และตรวจสอบได้ รวมถึงกำหนดสิทธิของเจ้าของข้อมูล และหน้าที่ความรับผิดชอบขององค์กรในฐานะผู้ควบคุมข้อมูล (Data Controller) และผู้ประมวลผลข้อมูล (Data Processor)

หลักสูตรนี้ถูกออกแบบเพื่อให้ผู้บริหารและพนักงานทุกฝ่ายเข้าใจข้อกำหนด PDPA อย่างเป็นระบบ สามารถนำไปประยุกต์ใช้กับงานจริง ลดความเสี่ยงการละเมิดข้อมูลส่วนบุคคล และสร้างวัฒนธรรมองค์กรที่เคารพสิทธิข้อมูลอย่างมืออาชีพ

❍ วัตถุประสงค์การเรียนรู้

1. เพื่อให้เข้าใจแนวคิดและข้อกำหนดสำคัญของกฎหมาย PDPA ที่เกี่ยวข้องกับการทำงานจริงในองค์กร
2. เพื่อแยกประเภทข้อมูลส่วนบุคคลและข้อมูลอ่อนไหว (Sensitive Data) พร้อมประเมินความเสี่ยงการใช้งานได้
3. เพื่อให้เข้าใจบทบาทหน้าที่ขององค์กรและบุคลากร เช่น Data Controller / Data Processor รวมถึงหน้าที่ของผู้เกี่ยวข้อง
4. เพื่อให้ปฏิบัติงานด้านการเก็บ ใช้ เปิดเผย และจัดเก็บข้อมูลส่วนบุคคลได้อย่างถูกต้องตามหลักการ PDPA
5. เพื่อจัดทำแนวทางป้องกันและรับมือเหตุข้อมูลรั่วไหล (Data Breach) และเตรียมความพร้อมให้ตรวจสอบได้

❍ เนื้อหาหลักสูตร

1. พื้นฐาน PDPA และสิ่งที่องค์กรต้องเข้าใจให้ตรงกัน

- PDPA คืออะไร และทำไมทุกหน่วยงานต้องเกี่ยวข้อง
- ความหมายสำคัญที่ต้องรู้
  - ข้อมูลส่วนบุคคล (Personal Data)
  - ข้อมูลอ่อนไหว (Sensitive Personal Data)
  - เจ้าของข้อมูล (Data Subject)
  - ผู้ควบคุมข้อมูล / ผู้ประมวลผลข้อมูล
- หลักการจัดการข้อมูลส่วนบุคคลที่ถูกต้อง (Principles)
- ความเสี่ยงหากไม่ปฏิบัติตาม PDPA (ภาพรวมผลกระทบต่อองค์กร)
- กิจกรรม (Workshop) : PDPA Quick Check: ตัวอย่างข้อมูล “อะไรคือ Personal Data / Sensitive Data” ให้ผู้เรียนช่วยกันแยกประเภท

2. ฐานกฎหมาย การขอความยินยอม และการใช้ข้อมูลอย่างถูกต้อง

- แนวทางการใช้ข้อมูลอย่างถูกต้องตาม PDPA
- ฐานกฎหมายในการประมวลผลข้อมูล (Lawful Basis) และแนวทางเลือกใช้ให้เหมาะสม
- Consent ที่ถูกต้องควรเป็นอย่างไร
- ความแตกต่างระหว่าง Consent กับการใช้ฐานกฎหมายอื่น
- แนวทางแจ้งรายละเอียดการเก็บข้อมูล (Privacy Notice)
- ความเสี่ยงที่องค์กรพบบ่อย เช่น
  - เก็บข้อมูลเกินจำเป็น
  - ใช้ข้อมูลผิดวัตถุประสงค์
  - ส่งต่อข้อมูลให้บุคคลภายนอกโดยไม่มีข้อกำหนด
- กิจกรรม (Workshop): วิเคราะห์กรณีศึกษา : “กรณีนี้ควรขอ Consent หรือใช้ฐานกฎหมายใด?” พร้อมเหตุผล

3. การบริหารข้อมูลส่วนบุคคลในกระบวนการทำงานจริงของแต่ละฝ่าย

- ตัวอย่างการจัดการข้อมูลส่วนบุคคลในแต่ละหน่วยงาน
  - HR: ข้อมูลสมัครงาน ประวัติพนักงาน สุขภาพ สวัสดิการ
  - Sales/Marketing: ลูกค้า Lead เบอร์โทร อีเมล กลุ่มเป้าหมาย
  - Customer Service: การร้องเรียน การบันทึกเสียง/ภาพ
  - Purchasing/Procurement: ข้อมูลคู่ค้า ผู้รับเหมา
  - IT: ระบบจัดเก็บ การเข้าถึง Password / Log
- หลักการ “Need to Know / Least Privilege”
- การจัดการเอกสารและไฟล์ข้อมูลส่วนบุคคลให้ปลอดภัย

- เอกสารกระดาษ
- ไฟล์ในคอมพิวเตอร์/ระบบแชร์
- กลุ่มไลน์/อีเมล

- แนวคิด Data Minimization & Data Retention
- แนวทางทำ Data Mapping แบบง่ายเพื่อเห็นข้อมูลขององค์กร
- กิจกรรม (Workshop) : ทำ “Data Mapping แบบย่อ” จากงานจริงของผู้เรียน (เก็บอะไร ใช้ทำอะไร เก็บที่ไหน ใครเข้าถึงได้)

4. สิทธิของเจ้าของข้อมูล การจัดการคำร้อง และการรับมือเหตุข้อมูลรั่วไหล

- สิทธิของเจ้าของข้อมูลที่องค์กรต้องรู้และปฏิบัติได้
  - ขอเข้าถึงข้อมูล
  - ขอแก้ไข
  - ขอให้ลบ/ทำลาย
  - ถอนความยินยอม
  - คัดค้านการประมวลผล
- แนวทางการรับเรื่องและการตอบสนองคำร้องอย่างเหมาะสม
- แนวคิด Data Breach คืออะไร และความเสี่ยงที่พบจริง
- ขั้นตอนการรับมือเมื่อเกิดเหตุข้อมูลรั่วไหล
  - ขอแจ้งใครก่อน
  - กักกันข้อมูล/จำกัดความเสียหาย
  - สรุปเหตุการณ์และป้องกันซ้ำ
- สรุปแนวทางสร้างวัฒนธรรมองค์กรด้าน PDPA
- กิจกรรม (Workshop) : Tabletop Simulation: จำลองเหตุการณ์ข้อมูลรั่วไหล 1 เคส และกำหนด “การตอบสนองภายใน 1 ชั่วโมงแรก”

❍ **วิทยากร** อาจารย์ ดร.พลกฤต โสลาพากุล

❍ **หลักสูตรนี้เหมาะสำหรับ** ผู้จัดการฝ่าย ผู้ช่วยผู้จัดการฝ่าย หัวหน้าแผนก หัวหน้าหน่วย และเจ้าหน้าที่ - แต่ละฝ่าย (ทุกหน่วยงานที่เกี่ยวข้องกับการจัดเก็บข้อมูลส่วนบุคคล)

❍ **ระยะเวลาการอบรม 1 วัน (09.00 – 16.00 น.)**

❍ **รูปแบบการฝึกอบรม**

1. การบรรเชิงโต้ตอบ (Interactive Lecture)
2. Case Study จากสถานการณ์จริงขององค์กร
3. Workshop แบบกลุ่ม (Data Mapping / Consent / Incident Response)
4. ถาม–ตอบปัญหาจริง (Q&A)
5. แบบทดสอบก่อนและหลังอบรม (Pre-Test / Post-Test)