มาตราการเชิงองค์กร

การรักษาความปลอดภัยข้อมูลส่วนบุคคล

กองมรดกภูมิปัญญาทางวัฒนธรรม

วัตถุประสงค์

1. กำหนดมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล
2. กำหนดแนวปฏิบัติให้เป็นไปตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA)
3. สร้างความเชื่อมั่นแก่เจ้าของข้อมูล
4. ป้องกันความเสี่ยง การละเมิด และข้อมูลรั่วไหล
5. เสริมความรู้ความเข้าใจแก่ข้าราชการและเจ้าหน้าที่

ขอบเขตของมาตราการ

1. ครอบคลุมหน่วยงานในกองมรดกภูมิปัญญาทางวัฒนธรรม
2. ใช้เป็นแนวทางจัดทำระเบียบและขั้นตอนปฏิบัติงานด้าน PDPA

หลักการทั่วไป

1. เก็บข้อมูลเท่าที่จำเป็น ตามวัตถุประสงค์ที่กำหนด
2. ใช้หรือเปิดเผยข้อมูลด้วยความระมัดระวังและรับผิดชอบ
3. ต้องได้รับความยินยอมที่ถูกต้อง หรือมีฐานกฎหมาย
4. เคารพสิทธิของเจ้าของข้อมูล เช่น เข้าถึง แก้ไข คัดค้าน ถอนความยินยอม ลบ หรือทำลายข้อมูล

มาตรการรักษาความปลอดภัยข้อมูล (CIA Triad)

ความลับ (Confidentiality)

- ควบคุมการเข้าถึงข้อมูลอิเล็กทรอนิกส์ จัดทำรหัสผ่านการเข้าถึงข้อมูลส่วนบุคคล ข้อมูลเอกสาร แต่งตั้งเจ้าหน้าที่ผู้เก็บรักษากุญแจและตู้เอกสารสำหรับการเก็บรักษาข้อมูลส่วนบุคคล
- เข้ารหัสข้อมูล กำหนดรหัสผ่านให้ยากต่อการเข้าถึงข้อมูลส่วนบุคคล โดยให้มีตัวอักษรผสมกับตัวเลขและสัญลักษณ์
- ป้องกันทางกายภาพ ใช้การล็อกตู้เอกสารและกำหนดรหัสผ่านสำหรับการเข้าสู่ระบบคอมพิวเตอร์
- นโยบายและการอบรมบุคลากร โดยให้เจ้าหน้าที่ผู้ควบคุมข้อมูลได้รับการฝึกอบรมและพัฒนาทักษะเกี่ยวกับนโยบายในการปกป้องข้อมูล
- ตรวจสอบการเข้าถึงข้อมูล เปลี่ยนรหัสผ่านทุก ๆ 3 เดือน และหมั่นตรวจสอบอีเมล์ของระบบในการเก็บรักษาข้อมูล เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ความถูกต้อง (Integrity)

- ถูกต้อง (Accuracy) : หมั่นตรวจทานความถูกต้องของข้อมูลให้ครบถ้วน
- ครบถ้วน (Completeness) : ตรวจสอบความครบถ้วนของเอกสารเป็นประจำและคอยตรวจทาน
- สอดคล้อง (Consistency) : ข้อมูลไม่เปลี่ยนแปลงไม่ว่าจะเข้าถึงด้วยวิธีใดหรือเวลาใดก็ตาม
- เชื่อถือได้ (Reliability) : อัปเดตข้อมูลส่วนบุคคลให้เป็นปัจจุบัน

ความพร้อม (Availability)

- Confidentiality (ความลับ): จำกัดการเข้าถึงเฉพาะผู้มีสิทธิ กำหนดให้เจ้าหน้าที่ควบคุมข้อมูลสามารถเข้าถึงข้อมูลได้ตามหน้าที่
- Integrity (ความสมบูรณ์) : ข้อมูลถูกต้องไม่ถูกแก้ไข หมั่นตรวจสอบความถูกต้องของข้อมูล
- Availability (ความพร้อมใช้งาน) : ระบบและข้อมูลพร้อมใช้งานเมื่อต้องการ

การป้องกันการละเมิดข้อมูล

ป้องกันการสูญหาย เข้าถึง ใช้ หรือเปิดเผยโดยมิชอบ ใช้มาตรการครบ 3 ด้าน ดังนี้

เชิงองค์กร
- นโยบาย
- บทบาท
- การอบรม

เชิงเทคนิค
- รหัสผ่าน
- เข้ารหัส
- กำหนดสิทธิ

เชิงกายภาพ
- ล็อกพื้นที่
- เก็บเอกสาร
- ปลอดภัย

การทบทวนมาตรการ

- ทบทวนเมื่อมีเหตุละเมิดหรือความจำเป็น
- วิเคราะห์สาเหตุ
- ปรับปรุงมาตรการให้รัดกุมยิ่งขึ้น
- แจ้ง สคส. และเจ้าของข้อมูล (หากมีความเสี่ยงสูง)

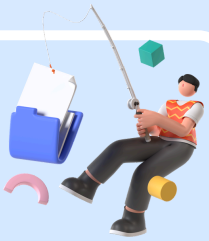
แนวทางการดำเนินการ เมื่อเกิด การละเมิดข้อมูลส่วนบุคคล

กองมรดกภูมิปัญญาและวัฒนธรรม

Data Breach คืออะไร

การละเมิดข้อมูลส่วนบุคคล คือ การที่ข้อมูลส่วนบุคคล

- สูญหาย
- ถูกเข้าถึง ถูกใช้
- ถูกเปลี่ยนแปลงหรือเปิดเผย

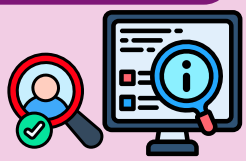


หน้าที่ของหน่วยงานเมื่อเกิดการละเมิด

- แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ภายใน 72 ชั่วโมง
- แจ้งเจ้าของข้อมูล เมื่อมีความเสี่ยงต่อสิทธิและเสรีภาพ
- มีมาตรการ แก้ไข ป้องกัน และบันทึกเหตุการณ์

การวิเคราะห์ความเสี่ยงข้อมูล (PDPA)

- ประเมิน **โอกาส** + **ผลกระทบ**
- เพื่อกำหนดมาตรการป้องกันที่เหมาะสม



ประโยชน์ของการวิเคราะห์ความเสี่ยง

- ลดความเสี่ยงทางกฎหมายและค่าปรับ
- สร้างความเชื่อมั่นให้ประชาชน
- อุดช่องโหว่ของระบบ เพิ่มความน่าเชื่อถือ

ตัวอย่างข้อมูลที่กองมรดกภูมิปัญญาทางวัฒนธรรมดูแล

ข้อมูลของ

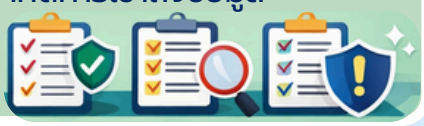
- คณะกรรมการ
- ผู้ทรงคุณวุฒิ
- ปราชญ์ชาวบ้าน

ข้อมูลที่เก็บ เช่น

- ชื่อ–นามสกุล
- ที่อยู่
- เบอร์โทรศัพท์
- สำเนาบัตรประชาชน /สำเนาบัญชีธนาคาร

มาตรการป้องกัน เช่น

- เก็บเอกสารในตู้ล็อก
- จำกัดการเข้าถึงข้อมูล



กระบวนการหลักในการจัดการความเสี่ยง

ประกอบด้วย 4 ขั้นตอนหลัก

1. ระบุและประเมินความเสี่ยง
2. ประเมินผลกระทบ
3. วางมาตรการป้องกันและแก้ไข
4. ทำ DPIA (Data Protection Impact Assessment)

ขั้นตอนเมื่อข้อมูลส่วนบุคคลถูกละเมิด

- ระบุลักษณะการละเมิด
- ประเมินผลกระทบ
- กำหนดการเยียวยาและแก้ไข
- จัดทำมาตรการป้องกันไม่ให้เกิดซ้ำ
- บันทึกเหตุการณ์ เป็นลายลักษณ์อักษร
- แจ้งเจ้าของข้อมูล (รายบุคคล / สาธารณะ)

การแจ้งเหตุ

แจ้ง สคส.

- ภายใน 72 ชั่วโมง
- หากล่าช้า ต้องชี้แจงเหตุผล (ไม่เกิน 15 วัน)

แจ้งเจ้าของข้อมูล

- แจ้งโดยไม่ชักช้า
- ระบุลักษณะเหตุ ผลกระทบ แนวทางเยียวยา และช่องทางติดต่อ DPO

ช่องทางร้องเรียน

- สายด่วน 1377
- โทร. 0-2141-3978-83
- อีเมล saraban@pdpc.or.th
- สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)