มาตราการเชิงองค์กร
การรักษาความปลอดภัยข้อมูลส่วนบุคคล
สถาบันวัฒนธรรมศึกษา

วัตถุประสงค์

1. กำหนดมาตรการรักษาความปลอดภัยข้อมูลส่วนบุคคล
2. ปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างเคร่งครัด
3. สร้างความเชื่อมั่นแก่เจ้าของข้อมูล
4. ป้องกันความเสี่ยง การละเมิด และการรั่วไหลของข้อมูล
5. คุ้มครองข้อมูลประชาชน ข้าราชการ และเจ้าหน้าที่

ขอบเขตของมาตราการ

1. ครอบคลุมหน่วยงานในสถาบันวัฒนธรรมศึกษา
2. หน่วยงานในสังกัดต้องนำไปใช้เป็นแนวทางในการจัดทำระเบียบและขั้นตอนการปฏิบัติงานด้านข้อมูลส่วนบุคคล

หลักการทั่วไป

1. เก็บข้อมูลเท่าที่จำเป็น ตามวัตถุประสงค์ที่กำหนด
2. ข้อมูลถูกต้อง ครบถ้วน เป็นปัจจุบัน
3. การเก็บ ใช้ เปิดเผย ต้องมีความยินยอมหรือฐานกฎหมายรองรับ
4. ดำเนินการด้วยความระมัดระวังและรับผิดชอบ

มาตรการรักษาความปลอดภัยข้อมูล (CIA Triad)

ความลับ (Confidentiality)

- ควบคุมการเข้าถึง 1. ข้อมูลอิเล็กทรอนิกส์ กำหนดรหัสผ่านที่รัดกุม และมีการเปลี่ยนรหัสตามรอบเวลา การล็อกหน้าจออัตโนมัติ 2. ข้อมูลกระดาษ จัดเก็บในตู้เอกสารที่ล็อกได้ จำกัดผู้ดูแลเฉพาะผู้ได้รับการมอบหมาย
- เข้ารหัสข้อมูล กำหนดรหัสการเข้าถึงข้อมูลที่มีเฉพาะบุคลากร สวศ. เท่านั้น
- ป้องกันทางกายภาพ ควบคุมการเข้าออกสถานที่และพื้นที่จัดเก็บข้อมูลด้วยบัตรผ่าน จำกัดสิทธิ์เฉพาะผู้เกี่ยวข้อง ติดตั้งกล้องวงจรปิด จัดเก็บเอกสารและอุปกรณ์ในสถานที่ที่มีความปลอดภัย และกำหนดวิธีการทำลายข้อมูลเมื่อพ้นระยะเวลาการเก็บรักษา
- นโยบายและการอบรมบุคลากร จัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ /นโยบายการใช้งานอุปกรณ์ /การจัดชั้นความลับของข้อมูล การฝึกอบรมการจัดการข้อมูลส่วนบุคคล ตามหลักของ PDPA
- ตรวจสอบการเข้าถึงข้อมูล ตรวจสอบสิทธิผู้ใช้เป็นระยะ ตรวจสอบการยืม–คืนเอกสาร ตรวจสอบการทำลาย

ความถูกต้อง (Integrity)

กำหนดขั้นตอนตรวจสอบความถูกต้องของข้อมูลก่อนและหลังการบันทึก ให้กรอกข้อมูลให้ครบถ้วนก่อนบันทึก มีระบบแจ้งเตือนเมื่อข้อมูลไม่สมบูรณ์ และมีการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อป้องกันข้อมูลสูญหาย รวมทั้งกำหนดมาตรฐานฐานข้อมูลเดียวกัน ควบคุมสิทธิการเข้าถึงและการแก้ไขข้อมูล พร้อมตรวจสอบและประเมินคุณภาพข้อมูลเป็นระยะ เพื่อให้ข้อมูลถูกต้องและน่าเชื่อถือ

ความพร้อม (Availability)

- Confidentiality (ความลับ) : จำกัดการเข้าถึงข้อมูลเฉพาะผู้มีสิทธิ์ โดยกำหนดสิทธิตามหน้าที่ ใช้รหัสผ่านและการยืนยันตัวตน พร้อมบันทึกการเข้าใช้งานเพื่อตรวจสอบได้
- Integrity (ความสมบูรณ์ของข้อมูล) : ควบคุมการแก้ไขข้อมูลเฉพาะผู้ได้รับอนุญาต ตรวจสอบความถูกต้องของข้อมูล และสำรองข้อมูลเป็นประจำ
- Availability (ความพร้อมใช้งาน) : จัดทำแผนสำรองและแผนกู้คืนระบบ เพื่อให้ระบบและข้อมูลสามารถกลับมาใช้งานได้เมื่อเกิดเหตุฉุกเฉิน

การป้องกันการละเมิดข้อมูล

ป้องกันการสูญหาย เข้าถึง ใช้ หรือเปิดเผยโดยมิชอบ ใช้มาตรการครบ 3 ด้าน ได้แก่

เชิงองค์กร	เชิงเทคนิค	เชิงกายภาพ
• นโยบาย	• รหัสผ่าน	• ล็อกพื้นที่
• บทบาท	• เข้ารหัส	• เก็บเอกสาร
• การอบรม	• กำหนดสิทธิ	• ปลอดภัย

การทบทวนมาตรการ

- แจ้ง สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)
- แจ้งเจ้าของข้อมูล (กรณีมีความเสี่ยงสูง)
- ตรวจสอบสาเหตุ และปรับปรุงมาตรการ
- นำไปพัฒนากระบวนการทำงานให้รัดกุมยิ่งขึ้น

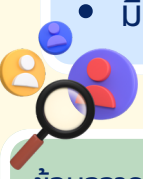
แนวทางการดำเนินการ
เมื่อเกิด การละเมิดข้อมูลส่วนบุคคล
สถาบันวัฒนธรรมศึกษา

ความหมายของการละเมิดข้อมูลส่วนบุคคล

การละเมิดข้อมูลส่วนบุคคล (Data Breach) คือ การที่ข้อมูลส่วนบุคคล สูญหาย ถูกเข้าถึง ใช้ เปลี่ยนแปลง หรือเปิดเผยโดยไม่ได้รับอนุญาต อาจเกิดจากความตั้งใจ ความประมาท หรืออุบัติเหตุ

หน้าที่ของหน่วยงานเมื่อเกิดการละเมิด

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



ตัวอย่างข้อมูลที่สถาบันวัฒนธรรมศึกษาดูแล

ข้อมูลจากกิจกรรมและกระบวนงาน เช่น
- การเสนอคำของบประมาณด้านวิจัย
- การขอเช่าใช้สถานที่ศูนย์วัฒนธรรมแห่งประเทศไทย
- การคัดเลือกปูชนียบุคคลด้านภาษาไทย
- การคัดเลือกครูอาวุโสดนตรีไทย

กลุ่มเจ้าของข้อมูล เช่น
- นักวิจัย
- ผู้เช่าสถานที่
- นักเรียน/นักศึกษา
- ครูอาวุโส

มาตรการป้องกัน เช่น
- ตั้งรหัสผ่านที่รัดกุม
- เปลี่ยนรหัสผ่านตามรอบเวลา
- ล็อกหน้าจออัตโนมัติ
- เก็บเอกสารในตู้ที่ล็อกได้

การวิเคราะห์ความเสี่ยงข้อมูล (PDPA)

- ลักษณะของข้อมูล (ข้อมูลทั่วไป / ข้อมูลอ่อนไหว)
- ปริมาณข้อมูล กลุ่มเจ้าของข้อมูล เช่น เด็ก ผู้สูงอายุ
- ลักษณะเหตุการณ์ เช่น ถูกแฮก ระบบล่ม
- ผลกระทบที่อาจเกิดขึ้น
- มาตรการความปลอดภัยที่มีอยู่

ประโยชน์ของการวิเคราะห์ความเสี่ยง

- ลดความเสี่ยงทางกฎหมายและค่าปรับ
- สร้างความน่าเชื่อถือให้หน่วยงาน
- ค้นหาช่องโหว่ด้านความปลอดภัย
- เพิ่มความเชื่อมั่นต่อองค์กร

กระบวนการหลักในการจัดการความเสี่ยง

1.ระบุและประเมินความเสี่ยง
2.วางแผนมาตรการป้องกัน/เยียวยา
3.ทำ DPIA หากมีความเสี่ยงสูง

ขั้นตอนเมื่อข้อมูลส่วนบุคคลถูกละเมิด

- ระงับการเข้าถึงข้อมูลทันที
- ตรวจสอบสาเหตุและขอบเขตความเสียหาย
- แจ้งเจ้าของข้อมูลและหน่วยงานกำกับดูแลภายใน 72 ชั่วโมง
- เยียวยาความเสียหายแก่เจ้าของข้อมูล
- ปรับปรุงมาตรการความปลอดภัย เพื่อป้องกันไม่ให้เกิดซ้ำ
- ติดตามและรายงานผลการแก้ไข

การแจ้งเหตุ

เมื่อเกิดการละเมิดข้อมูลส่วนบุคคล
- ต้องแจ้ง สคส. ภายใน 72 ชั่วโมง หากมีความเสี่ยงสูง
- ต้องแจ้ง เจ้าของข้อมูลส่วนบุคคล ด้วย

ข้อมูลที่ต้องแจ้ง เช่น
- ลักษณะการละเมิด
- ผลกระทบที่อาจเกิดขึ้น
- แนวทางการแก้ไขและเยียวยา

ช่องทางร้องเรียน (สำหรับเจ้าของข้อมูล)

- โทรศัพท์ : 1377 / 0-2141-3978-83
- อีเมล : saraban@pdpc.or.th
- สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)