การกำกับประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคล

---

1. ความเป็นมา

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ได้มีผลบังคับใช้เพื่อยกระดับการคุ้มครองข้อมูลส่วนบุคคลของประชาชนทุกกลุ่มอย่างเป็นระบบ โดยเฉพาะหน่วยงานของรัฐที่เกี่ยวข้องกับการบริหารจัดการข้อมูลส่วนบุคคลโดยตรง เช่น ข้อมูลของบุคลากร ข้อมูลคู่สัญญา หรือข้อมูลการเงินต่าง ๆ

สำนักงานโครงการ TO BE NUMBER ONE กรมสุขภาพจิต การดำเนินงานด้านงานบุคคล การเงิน และพัสดุ ซึ่งเกี่ยวข้องกับข้อมูลส่วนบุคคลหลายประเภท จึงจำเป็นต้องดำเนินการประเมินความเสี่ยง เพื่อให้มั่นใจได้ว่ามีมาตรการในการป้องกันและควบคุมที่เพียงพอ ลดโอกาสในการละเมิดสิทธิของเจ้าของข้อมูล และสร้างความเชื่อมั่นในกระบวนการทำงานของหน่วยงาน

2. วัตถุประสงค์

- เพื่อประเมินระดับความเสี่ยงที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในหน่วยงาน
- เพื่อกำหนดแนวทางในการจัดการความเสี่ยงให้เหมาะสมกับระดับความเสี่ยงที่พบ
- เพื่อให้การดำเนินงานด้านข้อมูลส่วนบุคคลของสำนักงานฯสอดคล้องกับกฎหมาย PDPA
- เพื่อสร้างวัฒนธรรมการทำงานที่ตระหนักถึงการคุ้มครองข้อมูลส่วนบุคคลในทุกกระบวนงาน

3. ขอบเขต

การประเมินความเสี่ยงฉบับนี้ครอบคลุมกิจกรรมต่าง ๆ ภายในสำนักงานโครงการ TO BE NUMBER ONE ที่เกี่ยวข้องกับข้อมูลส่วน บุคคล ได้แก่

- การเก็บข้อมูลของบุคลากรภายในหน่วยงาน
- การจัดซื้อจัดจ้าง และการบริหารงบประมาณ
- ข้อมูลการรับสมัครงาน ค่าตอบแทน และสวัสดิการต่าง ๆ
- การเก็บรักษาและการทำลายเอกสารที่มีข้อมูลส่วนบุคคล
- การส่งต่อ / เปิดเผยข้อมูลให้กับหน่วยงานภายนอกหรือบุคคลที่สาม

4. การวิเคราะห์ความเสี่ยง

4.1 ประเภทความเสี่ยงที่พิจารณา

- ความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- ความเสี่ยงจากการจัดเก็บข้อมูลโดยไม่มีมาตรการป้องกัน
- ความเสี่ยงจากการส่งหรือเปิดเผยข้อมูลผ่านช่องทางที่ไม่ปลอดภัย
- ความเสี่ยงจากการขาดนโยบายหรือแนวทางปฏิบัติที่ชัดเจน
- ความเสี่ยงจากการเก็บรักษาข้อมูลเกินระยะเวลาที่จำเป็น
- ความเสี่ยงจากการใช้ข้อมูลส่วนบุคคลของบุคคลที่สามโดยไม่ได้รับความยินยอม
- ความเสี่ยงจากการละเลยการทำลายข้อมูลอย่างปลอดภัย

4.2 ตารางความเสี่ยง

โดยใช้ โอกาสเกิด (Likeihood) และ ผลกระทบ (Impact) เป็นเกณฑ์

ผลกระทบ / โอกาส	1 (น้อยมาก)	2 (น้อย)	3 (ปานกลาง)	4 (สูง)	5 (สูงมาก)
5 (สูงมาก)	ปานกลาง	สูง	สูง	วิกฤติ	วิกฤติ
4 (สูง)	ปานกลาง	ปานกลาง	สูง	สูง	วิกฤติ
3 (ปานกลาง)	ต่ำ	ปานกลาง	ปานกลาง	สูง	สูง
2 (น้อย)	ต่ำ	ต่ำ	ปานกลาง	ปานกลาง	สูง
1 (น้อยมาก)	ต่ำ	ต่ำ	ต่ำ	ปานกลาง	ปานกลาง

4.3 รายการความเสี่ยง และการจัดระดับ

ลำดับ	รายการความเสี่ยง	โอกาส (1-5)	ผลกระทบ (1-5)	ระดับความเสี่ยง	หมายเหตุ
1	ข้อมูลการรับสมัครงานหรือบัญชีธนาคารรั่วไหลจากการเข้าถึงโดยไม่ได้รับอนุญาต	4	5	20 (วิกฤติ)	ต้องควบคุมสิทธิการเข้าถึงอย่างเข้มงวด
2	การส่งข้อมูลส่วนบุคคลผ่านช่องทางที่ไม่ปลอดภัย เช่น Line หรืออีเมลส่วนตัว	4	4	16 (สูง)	ควรจำกัดการใช้งานช่องทางที่ไม่ปลอดภัย
3	เอกสารที่มีข้อมูลส่วนบุคคลถูกทิ้งโดยไม่ทำลายอย่างปลอดภัย	3	4	12 (สูง)	ต้องมีแนวทางจัดการเอกสารอย่างปลอดภัย
4	ขาดนโยบายหรือแนวปฏิบัติเกี่ยวกับ PDPA ภายในสำนักฯ	5	4	20 (วิกฤติ)	จำเป็นต้องจัดทำนโยบายโดยเร่งด่วน
5	การเก็บข้อมูลส่วนบุคคลเกินระยะเวลาที่จำเป็นโดยไม่มีแนวทางลบข้อมูล	3	3	9 (ปานกลาง)	ควรจัดทำนโยบาย retention และลบข้อมูลเป็นระบบ

5. มาตรการจัดการความเสี่ยง

รายการความเสี่ยง	มาตรการจัดการความเสี่ยง
1. ข้อมูลการรับสมัครงานหรือบัญชีธนาคารรั่วไหลจากการเข้าถึงโดยไม่ได้รับอนุญาต	- กำหนดสิทธิ์การเข้าถึงตามหน้าที่ (Role - Based Access Control) - บันทึก log การเข้าถึงข้อมูลทุกครั้ง - ใช้รหัสผ่านและระบบยืนยันตัวตน (MFA)
2. การส่งข้อมูลส่วนบุคคลผ่านช่องทางที่ไม่ปลอดภัย	- ห้ามส่งข้อมูลผ่าน Line หรืออีเมลส่วนตัว - ใช้ระบบอีเมลภาครัฐที่มีการเข้ารหัส - พิจารณาใช้ระบบส่งไฟล์ผ่าน SFTP หรือ Secure Portal
3. เอกสารที่มีข้อมูลส่วนบุคคลถูกทิ้งโดยไม่ทำลายอย่างปลอดภัย	- จัดเตรียมเครื่องทำลายเอกสารไว้ประจำกอง - กำหนดขั้นตอนการทำลายเอกสารอย่างชัดเจน - อบรมเจ้าหน้าที่ให้ตระหนักถึงความสำคัญของข้อมูล
4. ขาดนโยบายหรือแนวปฏิบัติเกี่ยวกับ PDPA ภายในสำนักงานฯ	- จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลภายในกองฯ - จัดอบรม PDPA ให้เจ้าหน้าที่ประจำปี - มอบหมายผู้รับผิดชอบด้านข้อมูล (DPO / ผู้ประสานงาน)
5. การเก็บข้อมูลส่วนบุคคลเกินระยะเวลาที่จำเป็น	- จัดทำนโยบายการเก็บรักษาและลบข้อมูล (Retention Policy) - ตรวจสอบข้อมูลเป็นระยะ และลบข้อมูลที่หมดอายุ - ใช้ระบบแจ้งเตือนเมื่อครบกำหนดจัดเก็บข้อมูล

6. บทสรุป

จากการประเมินความเสี่ยงด้านการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานโครงการ TO BE NUMBER ONE พบว่า มีความเสี่ยงในหลายด้านที่ควรได้รับการจัดการอย่างเป็นระบบ โดยเฉพาะในเรื่องของการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตการจัดเก็บเอกสารโดยไม่มีมาตรการรักษาความปลอดภัย และการขาดแนวทางปฏิบัติที่ชัดเจน

สำนักงานโครงการ TO BE NUMBER ONE ควรดำเนินการปรับปรุงกระบวนการภายใน พร้อมจัดอบรมสร้างความรู้ความเข้าใจให้แก่เจ้าหน้าที่ทุกคน เพื่อให้การดำเนินงานเป็นไปตาม PDPA อย่างเคร่งครัด และสามารถลดความเสี่ยงที่จะเกิดขึ้นในอนาคต