

ผู้อำนวยการกองกลาง
เลขรับ 5316
วันที่ 11/4/66
เวลา 15.43 น.

กลุ่มสารบรรณ
เลขรับ 5891
วันที่ 11/4/66
เวลา 12.48

กระทรวงสาธารณสุข
เลขรับ 20345
วันที่ 17 มี.ย. 2566
เวลา 10.28

ด่วนที่สุด

ที่ ศค ๐๒๐๕/ว ๗๐๘๓



กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา

อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ

เขตหลักสี่ กรุงเทพฯ ๑๐๑๑๐

๑๐ เมษายน ๒๕๖๖

๒๕๖๖

ห้องรองปลัดกระทรวงฯ
นพ.พงศ์เกษม ไข่มุกด์
เลขรับ 8020/
วันที่ ๑๒ เม.ย. ๒๕๖๖
เวลา 16.06

ห้องปลัดกระทรวงฯ
นพ.โอภาส การย์กวินพงศ์
เลขรับ 2148
วันที่ ๑๒ เม.ย. ๒๕๖๖
เวลา 10.10

เลขที่ 3094
วันที่ 18 เม.ย. 2566
เวลา 8.42 น.

ห้อง ผอ.กยท
เลขที่ 4925
วันที่ 18/4/66
เวลา 04.01

กลุ่มดิจิทัลสุขภาพ
เลขรับ 167
วันที่ 19/4/66
เวลา 16.27

งานดิจิทัลสุขภาพ ๑
เลขรับ 76
วันที่ 19/4/66
เวลา 9.51

เรื่อง ขอความร่วมมือปฏิบัติตามแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในหน่วยงานของรัฐ
เรียน ปลัดกระทรวงสาธารณสุข
สิ่งที่ส่งมาด้วย สรุปรประชุมหารือแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในหน่วยงานของรัฐ
ตามที่ได้เกิดเหตุการณ์ผู้ไม่หวังดี (แฮกเกอร์) ละเมิดข้อมูลส่วนบุคคลของประชาชนและ
อ้างว่าข้อมูลประชาชนดังกล่าวรั่วไหลเป็นจำนวนมากจากหน่วยงานภาครัฐ ซึ่งเป็นที่ต้นตระหนักของสังคม
ในวงกว้าง ส่งผลต่อความเชื่อมั่นของหน่วยงานภาครัฐ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมจึงได้จัดประชุมหารือ
แนวทางการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลในหน่วยงานของรัฐ พร้อมหน่วยงานที่เกี่ยวข้อง เมื่อวันที่
๓ เมษายน ๒๕๖๖ โดยมีปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นประธานการประชุม นั้น

ในการนี้ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ขอเรียนสรุปแนวทางการดำเนินการและ
ขอความร่วมมือในการปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลในหน่วยงานของรัฐ ดังนี้

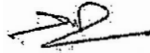
๑. ให้ตรวจสอบการเผยแพร่ข้อมูลส่วนบุคคล โดยเฉพาะการเผยแพร่ข้อมูลลงบนเว็บไซต์
แพลตฟอร์มหรือช่องทางต่าง ๆ (เช่น API หรือ Application Programming Interface) ของหน่วยงานภาครัฐ
ที่มีลักษณะเป็นการทั่วไปที่ทุกคนสามารถเข้าถึงได้ หากพบว่าหน่วยงานของท่านมีการเปิดเผยข้อมูลในลักษณะ
ดังกล่าว ขอให้ยุติการเผยแพร่ข้อมูลในทันที
๒. ให้ตรวจสอบระบบเทคโนโลยีสารสนเทศที่อยู่ในความครอบครองของหน่วยงาน และทำการ
ทดสอบเพื่อหาช่องโหว่ หรือการหลุดรั่วของข้อมูล ทั้งนี้ กรณี ตรวจสอบว่ามีข้อมูลรั่วหรือระบบเทคโนโลยีสารสนเทศ
มีช่องโหว่ ให้หน่วยงานเร่งปรับปรุงแก้ไข และรายงานมายังสำนักงานคณะกรรมการข้อมูลส่วนบุคคลโดยเร็ว
๓. จากกรณีปรากฏข่าวว่ามีการรั่วไหลของข้อมูลส่วนบุคคลประกอบด้วย ชื่อ-นามสกุล ที่อยู่
เบอร์โทรศัพท์ หมายเลขบัตรประชาชน จึงขอให้ทุกหน่วยงานพิจารณายกระดับการพิสูจน์ตัวตน (Identity
Proofing) โดยตรวจสอบข้อมูลของบุคคลกับหน่วยงานที่ออกหลักฐานแสดงตน เช่น ใช้เครื่องอ่านบัตรประชาชน
ที่อ่านข้อมูลจากชิป และหลีกเลี่ยงการใช้การพิสูจน์ตัวตนที่ใช้แค่ข้อมูลหน้าบัตรประชาชนและ Laser code
หลังบัตรเท่านั้น (กรณีมีการรั่วไหลของข้อมูล Laser code) รวมถึงให้ยกระดับการยืนยันตัวตน (Authentication)
ก่อนเข้าสู่ระบบของหน่วยงาน โดยใช้การยืนยันตัวตนแบบหลายปัจจัย เช่น กรอกรหัสผ่านร่วมกับรหัส OTP
ที่ส่งมายังโทรศัพท์ของผู้ให้บริการ หรือ เปรียบเทียบชีวมิติ (biometrics) และเรียกใช้กุญแจเข้ารหัส
(Cryptographic Software) ที่อยู่ในแอปพลิเคชัน

/หากต้องการ...

หากต้องการข้อมูลเพิ่มเติมสามารถประสานได้ที่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
๐ ๒๑๔๒ ๑๐๓๓ และสำนักงานปลัดกระทรวงฯ ๐ ๒๑๔๑ ๖๙๖๗ ทั้งนี้ กระทรวงฯ ได้แนบเอกสารสรุปการประชุม
หารือแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในหน่วยงานของรัฐ รายละเอียดตามสิ่งที่ส่งมาด้วย.

จึงเรียนมาเพื่อโปรดพิจารณา และขอได้โปรดแจ้งให้หน่วยงานในสังกัดของท่านให้ความร่วมมือ
ปฏิบัติตามแนวทางดังกล่าวต่อไปด้วย จะขอบคุณยิ่ง

ขอแสดงความนับถือ



(ศาสตราจารย์พิเศษวิศิษฏ์ วิศิษฏ์สรอรรถ)
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กองป้องกันและปราบปรามการกระทำคามผิดทางเทคโนโลยีสารสนเทศ
โทร ๐ ๒๑๔๑ ๖๙๖๗ โทรสาร ๐ ๒๑๔๓ ๘๐๓๔

สรุปประชุมหารือแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในหน่วยงานของรัฐ

วันจันทร์ที่ ๓ เมษายน ๒๕๖๖ เวลา ๑๑.๓๐ น.

ณ ห้องประชุม MDES1 ชั้น ๙ สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม กล่าวต่อที่ประชุมถึงความเป็นมากรณีการเกิดเหตุละเมิด
ตามที่มีการเผยแพร่ทางสื่อต่างๆ ซึ่งแจ้งแนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในหน่วยงาน
ของรัฐ เพื่อเร่งรัดให้หน่วยงานของรัฐตรวจสอบและทบทวนระบบเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐ
ให้เป็นไปตามมาตรฐานรักษาความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ ดำเนินการตามกฎหมายและแนวปฏิบัติ
ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูล/ข้อมูลส่วนบุคคล อย่างเคร่งครัด และเร่งรัดการใช้ Digital
ID เพื่อช่วยยกระดับการรักษาความมั่นคงปลอดภัยของข้อมูล/ข้อมูลส่วนบุคคล ของหน่วยงาน

ข้อเสนอแนะในการเร่งดำเนินการเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

๑. เร่งตรวจสอบว่ามีข้อมูลส่วนบุคคลในความรับผิดชอบของหน่วยงานเผยแพร่ในช่องทางสาธารณะหรือไม่ ถ้ามี
ให้ตรวจสอบว่าเป็นการเผยแพร่ตามเงื่อนไขในกฎหมายใดหรือไม่ และเปิดเผยข้อมูลเท่าที่จำเป็นหรือไม่ แต่
ถ้าเป็นเหตุการณ์ละเมิดฯ ต้องรีบแก้ไข และ แจ้งสำนักงานฯ
๒. เร่งตรวจสอบและแก้ไขช่องโหว่ของระบบสารสนเทศและฐานข้อมูลของหน่วยงาน เพื่อป้องกันการเข้าถึงโดย
มิชอบ โดยสามารถขอความสนับสนุนทางเทคนิคจาก สกมช. และ สคส.
๓. เร่งรัดการสร้างความรู้ให้กับบุคลากรของหน่วยงานในด้านการรักษาความมั่นคงปลอดภัยและการ
คุ้มครองข้อมูลส่วนบุคคล โดย สคส. และ สกมช. จะร่วมกันจัดฝึกอบรมหลักสูตรพิเศษให้แก่หน่วยงานภาครัฐ
ที่มีข้อมูลส่วนบุคคลของประชาชนจำนวนมาก
๔. ตรวจสอบย้อนหลังว่ามีผู้เข้าถึงระบบที่มีฐานข้อมูลส่วนบุคคลแบบไม่ปกติหรือไม่เป็นไปตามข้อกำหนดของ
หน่วยงานหรือไม่
๕. ควรจัดทำแผนและดำเนินการตามมาตรการการรักษาความมั่นคงปลอดภัยของระบบและข้อมูลส่วนบุคคล
เพิ่มเติม อาทิ
 - การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่งครั้ง
 - การประเมินความเสี่ยง (Risk Assessment) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่าง
มีประสิทธิภาพและต่อเนื่อง รวมถึงมีแนวทางการควบคุมและบริหารจัดการความเสี่ยงที่เหมาะสม
 - แผนการรับมือภัยคุกคามทางไซเบอร์และเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Incident Response Plan)
และการซึ่กซ้อม (Drill) จำลองเหตุการณ์ภัยคุกคาม ตามแผนการรับมือดังกล่าวอย่างสม่ำเสมอ
 - การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุละเมิดข้อมูลส่วนบุคคลตามแผนการ
วางแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)

ทั้งนี้ ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ได้สรุปแนวทางการดำเนินการและขอความร่วมมือในการปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลในหน่วยงานของรัฐ ดังนี้

๑. ให้ตรวจสอบการเผยแพร่ข้อมูลส่วนบุคคล โดยเฉพาะการเผยแพร่ข้อมูลลงบนเว็บไซต์ แพลตฟอร์มหรือช่องทางต่าง ๆ (เช่น API หรือ Application Programming Interface) ของหน่วยงานภาครัฐ ที่มีลักษณะเป็นการทั่วไป ที่ทุกคนสามารถเข้าถึงได้ หากพบว่าหน่วยงานของท่านมีการเปิดเผยข้อมูลในลักษณะดังกล่าว ขอให้ยุติการเผยแพร่ข้อมูลในทันที

๒. ให้ตรวจสอบระบบเทคโนโลยีสารสนเทศที่อยู่ในความครอบครองของหน่วยงาน และทำการทดสอบเพื่อหาช่องโหว่ หรือการหลุดรั่วของข้อมูล ทั้งนี้ กรณี ตรวจพบว่ามีข้อมูลรั่วหรือระบบเทคโนโลยีสารสนเทศมีช่องโหว่ ให้หน่วยงานเร่งปรับปรุงแก้ไข และรายงานมายังสำนักงานคณะกรรมการข้อมูลส่วนบุคคลโดยเร็ว

๓. จากกรณีปรากฏข่าวว่ามีการรั่วไหลของข้อมูลส่วนบุคคลประกอบด้วย ชื่อ-นามสกุล ที่อยู่ เบอร์โทรศัพท์ หมายเลขบัตรประชาชน จึงขอให้ทุกหน่วยงานพิจารณากระดับการพิสูจน์ตัวตน (Identity Proofing) โดยตรวจสอบข้อมูลของบุคคลกับหน่วยงานที่ออกหลักฐานแสดงตน เช่น ใช้เครื่องอ่านบัตรประชาชน ที่อ่านข้อมูลจากชิป และหลีกเลี่ยงการใช้การพิสูจน์ตัวตนที่ใช้แค่ข้อมูลหน้าบัตรประชาชนและ Laser code หลังบัตรเท่านั้น (กรณีมีการรั่วไหลของข้อมูล Laser code) รวมถึงให้ยกระดับการยืนยันตัวตน (Authentication) ก่อนเข้าสู่ระบบของหน่วยงาน โดยใช้การยืนยันตัวตนแบบหลายปัจจัย เช่น กรอกรหัสผ่านร่วมกับรหัส OTP ที่ส่งมายังโทรศัพท์ของผู้ให้บริการ หรือ เปรียบเทียบชีวมิติ (biometrics) และเรียกใช้กุญแจเข้ารหัส (Cryptographic Software) ที่อยู่ในแอปพลิเคชัน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

หน่วยงานของรัฐที่มีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะ เป็นข้อมูลของข้าราชการ พนักงานหรือประชาชนที่มารับบริการของรัฐ จะเป็นผู้ควบคุมข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ซึ่งมีหน้าที่ที่สำคัญตามมาตรา ๓๗ ดังนี้

(๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม รายละเอียดตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕)

(๒) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้รับใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ

(๓) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือตามเงื่อนไขที่กฎหมายกำหนด

(๔) แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าว และช้อยกเว้นให้เป็นไปตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

นอกจากนี้ ผู้ควบคุมข้อมูลส่วนบุคคลยังมีหน้าที่ที่ปรากฏในมาตราอื่น เช่น

(๑) การแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบถึงรายละเอียดและวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามมาตรา ๒๓

(๒) การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามเงื่อนไขที่กฎหมายกำหนดในหมวด ๒ การคุ้มครองข้อมูลส่วนบุคคล

(๓) การจัดทำบันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลสามารถตรวจสอบได้ตามมาตรา ๓๔

(๔) ในกรณีที่หน่วยงานของรัฐซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลได้ว่าจ้างหรือมอบหมายให้หน่วยงานอื่น ไม่ว่าจะ เป็นภาครัฐหรือเอกชน ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล หน่วยงานของรัฐซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลนั้นต้องจัดให้มีข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดในมาตรา ๔๐

(๕) การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา ๔๑ และ ๔๒

(๖) การดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามที่กฎหมายกำหนดในหมวด ๓ สิทธิของเจ้าของข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคลต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยขั้นต่ำ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

(๑) ครอบคลุมการเก็บรวบรวม ใช้และเปิดเผยข้อมูลส่วนบุคคล ไม่ว่าจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม

(๒) ต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

(๓) ต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่

- การระบุความเสี่ยงที่สำคัญที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศที่สำคัญ
- การป้องกันความเสี่ยงที่สำคัญที่อาจเกิดขึ้น
- การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

(๔) ต้องคำนึงถึงความสามารถในการดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง

(๕) สำหรับข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ มาตรการรักษาความมั่นคงปลอดภัยจะต้องครอบคลุมส่วนประกอบต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้อง และควรประกอบด้วยมาตรการป้องกันหลายชั้น เพื่อลดความเสี่ยงในกรณีที่มาตราการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์

(๖) มาตรการในส่วนที่เกี่ยวกับการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผยข้อมูลส่วนบุคคล อย่างน้อยต้องประกอบด้วยดำเนินการดังต่อไปนี้ที่เหมาะสมตามระดับความเสี่ยง

- การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญ (access control) ที่มีการพิสูจน์และยืนยันตัวตน และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งานที่เหมาะสม
- การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่เหมาะสม
- การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)
- การจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลัง (audit trails) ที่เหมาะสม

(๗) สร้างเสริมความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (privacy and security awareness)

(๘) ทบทวนมาตรการรักษาความมั่นคงปลอดภัย เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป หรือเมื่อมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

แนวปฏิบัติเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลสำหรับหน่วยงานซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล

“การละเมิดข้อมูลส่วนบุคคล” หมายความว่า การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจ หรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่อง หรืออุบัติเหตุ หรือเหตุอื่นใด

เมื่อหน่วยงานซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคลได้รับแจ้งข้อมูลในเบื้องต้นจากผู้ใด ไม่ว่าจะโดยทางวาจา เป็น หนังสือ หรือวิธีการอื่นทางอิเล็กทรอนิกส์ หรือผู้ควบคุมข้อมูลส่วนบุคคลทราบเอง ว่ามีหรือน่าจะเกิดเหตุการณ์ละเมิด ข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการ ดังต่อไปนี้

(๑) ประเมินความน่าเชื่อถือของข้อมูลดังกล่าว และตรวจสอบข้อเท็จจริงในเบื้องต้นโดยไม่ชักช้า ว่ามีเหตุอันควรเชื่อได้ว่าการละเมิดข้อมูลส่วนบุคคลหรือไม่ รวมทั้งประเมินความเสี่ยงที่การละเมิดข้อมูล ส่วนบุคคลดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

(๒) หากระหว่างการตรวจสอบข้อเท็จจริง พบว่ามีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของ บุคคล ให้ดำเนินการป้องกัน ระวัง หรือแก้ไขเพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุดหรือไม่ให้การละเมิดข้อมูล ส่วนบุคคลส่งผลกระทบเพิ่มเติมโดยทันที เท่าที่จะสามารถกระทำได้

(๓) หากมีเหตุอันควรเชื่อได้ว่าการละเมิดข้อมูลส่วนบุคคลจริง ให้ผู้ควบคุมข้อมูลส่วนบุคคล แจ้งเหตุการณ์ละเมิดแก่สำนักงานโดยไม่ชักช้าภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล

(๔) ในกรณีที่การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของ บุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับ แนวทางการเยียวยาโดยไม่ชักช้าด้วย

(๕) ดำเนินการตามมาตรการที่จำเป็นและเหมาะสมเพื่อระงับ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจาก เหตุการณ์ละเมิดข้อมูลส่วนบุคคลดังกล่าว รวมทั้งป้องกันและลดผลกระทบจากการเกิดเหตุการณ์ละเมิดข้อมูล ส่วนบุคคลในลักษณะเดียวกันในอนาคต

การแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงาน สามารถแจ้งเป็นลายลักษณ์อักษร หรือ แจ้งทางอีเมล saraban@pdpc.or.th โดยต้องระบุสาระสำคัญดังต่อไปนี้เท่าที่จะสามารถกระทำได้

(๑) ข้อมูลโดยสังเขปเท่าที่จะสามารถระบุได้เกี่ยวกับลักษณะและประเภทของการละเมิดข้อมูล ส่วนบุคคล โดยอาจบรรยายถึงลักษณะและจำนวนเจ้าของข้อมูลส่วนบุคคลหรือลักษณะและจำนวนรายการ (records) ของข้อมูลส่วนบุคคลที่เกี่ยวข้องกับการละเมิด

(๒) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีเจ้าหน้าที่ คุ้มครองข้อมูลส่วนบุคคล หรือชื่อ สถานที่ติดต่อ และวิธีการติดต่อของบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมาย ให้ทำหน้าที่ประสานงานและให้ข้อมูลเพิ่มเติม

(๓) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

(๔) ข้อมูลเกี่ยวกับมาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล หรือเยียวยาความเสียหาย โดยอาจใช้มาตรการทางบุคลากร กระบวนการ หรือเทคโนโลยี หรือมาตรการอื่นใดที่จำเป็นและเหมาะสม

ผู้ควบคุมข้อมูลส่วนบุคคลอาจขอให้สำนักงานพิจารณาถึงความผิดจากการแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลล่าช้ากว่า ๗๒ ชั่วโมงนับแต่ทราบเหตุได้ โดยให้ผู้ควบคุมข้อมูลส่วนบุคคลชี้แจงเหตุผล ความจำเป็นและรายละเอียดที่เกี่ยวข้องเพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ แต่จะต้องแจ้งแก่สำนักงานโดยเร็ว ไม่เกิน ๑๕ วันนับแต่ทราบเหตุ

หากผู้ควบคุมข้อมูลส่วนบุคคลได้ตรวจสอบข้อเท็จจริงแล้วพบว่า การละเมิดข้อมูลส่วนบุคคลดังกล่าวมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ผู้ควบคุมข้อมูลส่วนบุคคลแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลพร้อมสาระสำคัญดังต่อไปนี้ให้เจ้าของข้อมูลส่วนบุคคลที่ได้รับผลกระทบทราบเท่าที่จะสามารถกระทำ ได้โดยไม่ชักช้า

(๑) ข้อมูลโดยสังเขปเกี่ยวกับลักษณะของการละเมิดข้อมูลส่วนบุคคล

(๒) ชื่อ สถานที่ติดต่อ และวิธีการติดต่อของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลหรือบุคคลที่ผู้ควบคุมข้อมูลส่วนบุคคลมอบหมายให้ทำหน้าที่ประสานงาน

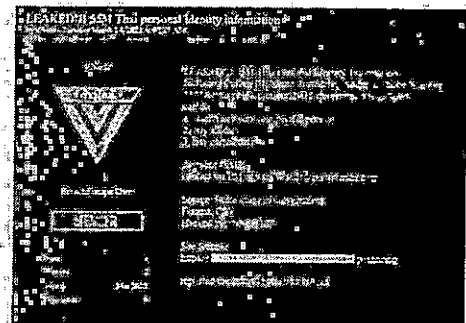
(๓) ข้อมูลเกี่ยวกับผลกระทบที่อาจเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคลจากเหตุการณ์ละเมิด

(๔) แนวทางการเยียวยาความเสียหายของเจ้าของข้อมูลส่วนบุคคล และข้อมูลโดยสังเขปเกี่ยวกับ มาตรการที่ผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือจะใช้เพื่อป้องกัน ระวัง หรือแก้ไขเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

แนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในหน่วยงานของรัฐ

ความเป็นมา: ข่าวเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

- ❑ เว็บไซต์ 9near.org ประกาศขายข้อมูลคนไทย ๕๕ ล้านราย วันที่ ๒๙ มีนาคม ๒๕๖๖ โดยมีลิงก์ดาวน์โหลดไฟล์ข้อมูล และระบุข้อความในลักษณะข่มขู่ให้ผู้คิดว่าข้อมูลของตนรั่วไหล ติดต่อกลับก่อนวันที่ ๕ เมษายน ๒๕๖๖

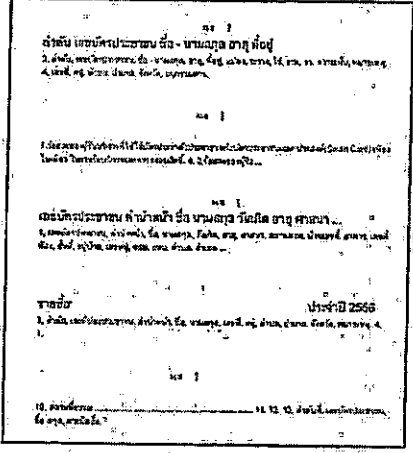
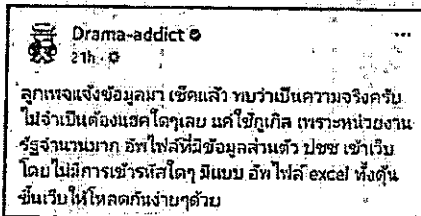


- ❑ ดศ. ร่วมกับหน่วยงานที่เกี่ยวข้อง เร่งดำเนินการตรวจสอบข้อเท็จจริง และประสานผู้ให้บริการเพื่อขอปิดกั้นเว็บไซต์ 9near.org

แนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในหน่วยงานของรัฐ

- ❑ เพจ Drama-addict ได้เผยแพร่ข้อความว่ามีหน่วยงานภาครัฐ อัปโหลดไฟล์ที่มีข้อมูลส่วนบุคคลเข้าสู่เว็บ โดยไม่มีการเข้ารหัสใดๆ (๓๑ มีนาคม ๒๕๖๖)

- ❑ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) ร่วมกับ สำนักงานคณะกรรมการการศึกษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้สุ่มตรวจโดยการค้นหาข้อมูลใน Google พบว่ามีหน่วยงานภาครัฐ เก็บไฟล์ข้อมูลส่วนบุคคลของประชาชนที่สามารถค้นหาและดาวน์โหลดได้ใน Public Domain



แนวทางการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลในหน่วยงานของรัฐ

- แนวทางการดำเนินการเพื่อเร่งรัดให้ระบบเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐ เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูล/ข้อมูลส่วนบุคคล อย่างมีประสิทธิภาพ
- แนวทางการดำเนินการตามกฎหมายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูล/ข้อมูลส่วนบุคคล อย่างเคร่งครัด
- แนวทางการทำงานร่วมกันและการช่วยเหลือสนับสนุนด้านการรักษาความมั่นคงปลอดภัยของข้อมูล/ข้อมูลส่วนบุคคล โดยหน่วยงานที่เกี่ยวข้อง
- แนวทางการเร่งรัดการใช้ Digital ID เพื่อช่วยยกระดับการรักษาความมั่นคงปลอดภัยของข้อมูล/ข้อมูลส่วนบุคคล ของหน่วยงาน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

ผู้ควบคุมข้อมูลส่วนบุคคล ที่เป็นหน่วยงานภาครัฐ มีหน้าที่ ที่สำคัญ ตามมาตรา ๓๗ แห่ง พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ดังนี้

๑. จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
๒. แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายใน ๗๒ ชั่วโมงนับแต่ทราบเหตุ เท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่มีการละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย
๓. ในกรณีที่ต้องแชร์ข้อมูลส่วนบุคคลให้บุคคลหรือนิติบุคคลอื่น ต้องมีมาตรการเพื่อป้องกันมิให้ผู้อื่นดังกล่าว ใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ
๔. จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือตามเงื่อนไขที่กฎหมายกำหนด

มาตรการรักษาความมั่นคงปลอดภัย (ที่สำคัญ)

๑. ต้องมีมาตรการเกี่ยวกับการ Access Control เพื่อควบคุมการเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข ลบ หรือเปิดเผย ข้อมูลส่วนบุคคล อย่างเหมาะสมตามระดับความเสี่ยง และสามารถตรวจสอบย้อนกลับได้
๒. สร้างเสริมความตระหนักรู้ด้านการคุ้มครองข้อมูลส่วนบุคคลและการรักษาความมั่นคงปลอดภัย (Privacy and Security Awareness) ให้แก่บุคลากรของหน่วยงาน
๓. มีการระบุความเสี่ยงของภัยและเหตุการณ์ที่อาจเกิดขึ้น มีการป้องกัน ตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล รวมถึง การเผชิญเหตุ และการรักษาและฟื้นฟู เมื่อเกิดความเสียหาย
๔. ต้องคำนึงถึงความสามารถในการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของข้อมูลส่วนบุคคลไว้ได้อย่างเหมาะสมตามระดับความเสี่ยง
๕. ต้องประกอบด้วยมาตรการเชิงองค์กร (Organizational Measures) และมาตรการเชิงเทคนิค (Technical Measures) ที่เหมาะสม รวมถึงมาตรการทางกายภาพ (Physical Measures) ที่จำเป็นด้วย

**แนวปฏิบัติเมื่อเกิดเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
สำหรับหน่วยงานซึ่งเป็นผู้ควบคุมข้อมูลส่วนบุคคล**

๑. ประเมินความน่าเชื่อถือของข้อมูล และตรวจสอบข้อเท็จจริงเกี่ยวกับการละเมิดฯ โดยไม่ชักช้า ว่ามีเหตุอันควรเชื่อได้ว่าการละเมิดฯ หรือไม่
๒. ป้องกัน ระบุ หรือแก้ไข เพื่อให้การละเมิดข้อมูลส่วนบุคคลสิ้นสุด โดยเฉพาะอย่างยิ่งกรณีความเสียหายสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล ต้องดำเนินการแก้ไขโดยทันทีหรือเร็วที่สุด
๓. แจ้งเหตุการณ์ละเมิดฯ แก่สำนักงานฯ โดยไม่ชักช้าภายใน ๗๒ ชั่วโมง นับแต่ทราบเหตุ เมื่อพิจารณาแล้วเห็นว่า มีเหตุอันควรเชื่อได้ว่าการละเมิดฯ จริง
๔. แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบ พร้อมแนวทางการเยียวยา โดยไม่ชักช้า กรณีที่การละเมิดฯ มีความเสียหายสูงที่จะมีผลกระทบต่อสิทธิเสรีภาพของบุคคล
๕. ดำเนินการตามมาตรการที่จำเป็นและเหมาะสม เพื่อระบุ ตอบสนอง แก้ไข หรือฟื้นฟูสภาพจากเหตุการณ์ละเมิดฯ

การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

แจ้งเป็นลายลักษณ์อักษร หรือแจ้งทางอีเมล saraban@pdpc.or.th ภายใน ๗๒ ชั่วโมง* นับแต่ทราบเหตุ โดยต้องระบุสาระสำคัญดังต่อไปนี้

๑. ข้อมูลโดยสังเขป เกี่ยวกับลักษณะและประเภทของการละเมิดฯ
๒. ชื่อ สถานที่ติดต่อ และวิธีการติดต่อ ของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
๓. ผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ละเมิดฯ
๔. ข้อมูลเกี่ยวกับมาตรการที่ใช้หรือจะใช้เพื่อป้องกัน ระบุ หรือแก้ไขเหตุการณ์ละเมิดฯ หรือเยียวยาความเสียหาย

* กรณีมีเหตุจำเป็นที่ทำให้แจ้งเหตุการละเมิดฯ ช้ากว่า ๗๒ ชั่วโมง นับแต่ทราบเหตุ ผู้ควบคุมข้อมูลส่วนบุคคล อาจขอให้สำนักงานฯ พิจารณายกเว้นความผิดได้ โดยให้ชี้แจงเหตุผลความจำเป็นและรายละเอียดที่เกี่ยวข้อง เพื่อแสดงให้เห็นว่ามีเหตุจำเป็นที่ไม่อาจหลีกเลี่ยงได้ โดยจะต้องแจ้งแก่สำนักงานฯ โดยเร็ว ไม่เกิน ๑๕ วันนับแต่ทราบเหตุ

ประเด็นขอความร่วมมือจากหน่วยงานของรัฐเพื่อดำเนินการโดยเร่งด่วน

ข้อเสนอแนะในการเร่งดำเนินการเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

๑. เฝ้าตรวจสอบว่ามีข้อมูลส่วนบุคคลในความรับผิดชอบของหน่วยงานเผยแพร่ในช่องทางสาธารณะหรือไม่ ถ้ามี ให้ตรวจสอบว่าเป็นการเผยแพร่ตามเงื่อนไขในกฎหมายใดหรือไม่ และเปิดเผยข้อมูลเท่าที่จำเป็นหรือไม่ แต่ถ้าเป็นเหตุการณ์ละเมิดฯ ต้องรีบแก้ไข และ แจ้งสำนักงานฯ
๒. เฝ้าตรวจสอบและแก้ไขช่องโหว่ของระบบสารสนเทศและฐานข้อมูลของหน่วยงาน เพื่อป้องกันการเข้าถึงโดยมิชอบ โดยสามารถขอความสนับสนุนทางเทคนิคจาก สกมช. และ สคส.
๓. เฝ้าระวังการสร้างความตระหนักรู้ให้กับบุคลากรของหน่วยงานในด้านการรักษาความมั่นคงปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคล โดย สคส. และ สกมช. จะร่วมกันจัดฝึกอบรมหลักสูตรพิเศษให้แก่หน่วยงานภาครัฐที่มีข้อมูลส่วนบุคคลของประชาชนจำนวนมาก
๔. ตรวจสอบย้อนหลังว่ามีผู้เข้าถึงระบบที่มีฐานข้อมูลส่วนบุคคลแบบไม่ปกติหรือไม่เป็นไปตามข้อกำหนดของหน่วยงานหรือไม่

ประเด็นขอความร่วมมือจากหน่วยงานของรัฐเพื่อดำเนินการโดยเร่งด่วน

๕. ควรจัดทำแผนและดำเนินการตามมาตรการการรักษาความมั่นคงปลอดภัยของระบบและข้อมูลส่วนบุคคลเพิ่มเติม อาทิ
 - การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่งครั้ง
 - การประเมินความเสี่ยง (Risk Assessment) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง รวมถึงมีแนวทางการควบคุมและบริหารจัดการความเสี่ยงที่เหมาะสม
 - แผนการรับมือภัยคุกคามทางไซเบอร์และเหตุการณ์ละเมิดข้อมูลส่วนบุคคล (Incident Response Plan) และการซึกซ้อม (Drill) จำลองเหตุการณ์ภัยคุกคาม ตามแผนการรับมือดังกล่าวอย่างสม่ำเสมอ
 - การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุละเมิดข้อมูลส่วนบุคคลตามแผนการวางแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)
๖. จัดตั้งคณะกรรมการ/คณะทำงานร่วมเพื่อกำกับดูแลให้หน่วยงานฯ มีการรักษาความมั่นคงปลอดภัยและการคุ้มครองข้อมูลส่วนบุคคลอย่างเข้มแข็ง ทั้งนี้ สคส. จะจัดตั้งทีมงานขึ้นมากภายใน สคส. เพื่อคอยสุ่มตรวจสอบเป็นระยะๆ ว่ามีการรั่วไหลของข้อมูลส่วนบุคคลประชาชนไปใน Public Domain หรือไม่