แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)
กรมฝนหลวงและการบินเกษตร

กรมฝนหลวงและการบินเกษตร กำหนดกรอบการทำงานเป็นขั้นตอนการปฏิบัติของผู้ควบคุมข้อมูล (Data Controller) โดยอ้างอิงจากมาตรา ๓๗ แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เรื่องหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล ซึ่งมีทั้งหมด ๕ ข้อ ดังนี้

มาตรา ๓๗ (๑) *จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไปเพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม ทั้งนี้ ให้เป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการประกาศกำหนด*

- มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)
- มาตรการป้องกันด้านเทคนิค (technical safeguard)
- มาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)

๑. มาตรการป้องกันด้านการบริหารจัดการ (administrative safeguard)

๑.๑ การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control) การจัดทำระบบการลงทะเบียนผู้ใช้งาน เพื่อตรวจสอบสิทธิการเข้าถึง พร้อมทั้งทบทวนสิทธิ์

๑.๑.๑ การกำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่ม
ผู้ดูแลระบบ
ผู้ใช้งานระบบ

๑.๑.๒ การทบทวนสิทธิ์
ลาออก
เปลี่ยนตำแหน่ง
โอน ย้าย
สิ้นสุดการจ้าง

๑.๒ ผู้ใช้งานระบบสารสนเทศต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บริหารของหน่วยงานนั้น

๑.๒.๑ ระบบสารสนเทศต้องมีการจัดแบ่งประเภทและความสำคัญ ลำดับชั้นความลับ และการเข้าถึงข้อมูล

๑.๒.๑.๑ จัดแบ่งลำดับชั้นความลับของข้อมูล
- ข้อมูลลับที่สุด
- ข้อมูลลับมาก

- ข้อมูลลับ
- ข้อมูลทั่วไป

๑.๒.๑.๒ จัดแบ่งระดับชั้นการเข้าถึง
- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ดูแลระบบ
- ระดับชั้นสำหรับผู้ปฏิบัติงาน
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

๑.๓ การกำหนดเวลาที่สามารถเข้าใช้งานระบบสารสนเทศ

๑.๓.๑ ระบบยืนยันตัวตนก่อนเข้าใช้งานระบบ

๑.๓.๒ สามารถเข้าใช้งานได้ตลอด ๒๔ ชั่วโมง ๗ วัน

๑.๓.๓ ยุติการใช้งานโดยการออกจากระบบโดยอัตโนมัติ เมื่อไม่มีการใช้งานในช่วงระยะเวลา ๑๐ นาที เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑.๔ แนวทางการควบคุมการเข้าถึง และการแบ่งระดับชั้นและสิทธิการเข้าถึง

๑.๔.๑ ระดับผู้ดูแลระบบ มีหน้าที่ในการควบคุมการเข้าถึงข้อมูล รวมไปถึงวิธีการทำลายข้อมูล

๑.๔.๒ ระดับเจ้าของข้อมูล มีหน้าที่ตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

๑.๔.๓ ระดับผู้ปฏิบัติงาน มีหน้าที่ในการบันทึก ตรวจสอบ ปรับปรุง และรายงานข้อมูล

๑.๔.๔ ระดับชั้นสำหรับผู้ใช้งานทั่วไป มีสิทธิในการใช้ข้อมูลตามสิทธิที่มอบให้เท่านั้น

๑.๕ การบริหารจัดการ การเข้าถึงของผู้ใช้งาน

๑.๕.๑ จัดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัย สารสนเทศ

๑.๕.๒ กำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน

๑.๕.๓ การบริหารจัดการสิทธิของผู้ใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม

๑.๕.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๑.๖ ขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน

๑.๖.๑ จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิ

๑.๖.๒ ระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน โดยกำหนดเป็นชื่อภาษาอังกฤษและตัวเลข

๑.๖.๓ ตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่

๑.๖.๔ เอกสารแบบฟอร์มแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

๑.๖.๕ การอนุญาตให้เข้าถึงระบบสารสนเทศ ต้องได้รับการอนุญาตจากผู้บริหาร หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๖.๖ หลักเกณฑ์ในการยกเลิกให้เข้าถึงระบบสารสนเทศเมื่อลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง

๑.๗ การบริหารจัดการสิทธิของผู้ใช้งาน

๑.๗.๑ กำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความ รับผิดชอบ

๑.๗.๒ การมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึงระบบสารสนเทศ

๑.๗.๓ บันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิของผู้ใช้งาน

๑.๘ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๑.๘.๑ การตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัยดังนี้

- ตัวเลข ตัวอักษร และตัวอักษรพิเศษ ไม่น้อยกว่าหรือเท่ากับ ๘ ตัวอักษร
- ไม่ใช้ชื่อ
- นามสกุลของตนเอง หรือบุคคลใกล้ชิดตน
- วัน เดือน ปีเกิด
- เบอร์โทรศัพท์
- คำศัพท์ที่ใช้ในพจนานุกรม

๑.๘.๒ ห้ามส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานทาง e-mail หรือช่องทางอื่นทางโซเชียล

๑.๘.๓ ให้ผู้ใช้งานเปลี่ยนรหัสผ่านทันทีหลังจากใช้รหัสผ่านชั่วคราวเข้าระบบ

๑.๘.๔ ไม่ให้รหัสผ่านกับผู้อื่น และ เปลี่ยนรหัสผ่านทุกๆ ๑๘๐ วันหรือตามการแจ้งเตือนจากผู้ดูแลระบบ

๑.๙ การรักษารหัสผ่านเพิ่มเติม

- การกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน ตามวิธีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน
- เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
- เก็บรหัสผ่านไว้เป็นความลับ ห้ามจดไว้ในที่เปิดเผย
- ห้ามให้โปรแกรมเข้าใช้งานบันทึกรหัสผ่าน
- กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน ให้ทำการเปลี่ยนรหัสผ่านโดย ทันที
- ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่าน ถี่กว่าผู้ใช้งานทั่วไป

๒. มาตรการป้องกันทางกายภาพ (physical safeguard) ในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (access control)

๒.๑ การป้องกันอุปกรณ์คอมพิวเตอร์ และระบบสารสนเทศ

๒.๑.๑ มีบัญชีควบคุมอุปกรณ์ที่ใช้งานเพื่อป้องกันการสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๑.๒ อุปกรณ์ที่ไม่มีการใช้งานต้องเก็บไว้ในที่ปลอดภัย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๑.๓ ต้องใส่รหัสผ่านก่อนเข้าใช้งานคอมพิวเตอร์

๒.๑.๔ ล็อคหน้าจอคอมพิวเตอร์หลังจากที่ไม่ได้ใช้งานเป็นเวลา ๑๐ นาที

๒.๑.๕ กำหนดให้ระบบสารสนเทศ ออกจากระบบอัตโนมัติเมื่อไม่ได้ใช้งานเป็นเวลา ๑๐ นาที

๒.๑.๖ ออกจากระบบสารสนเทศทันทีที่ใช้งานเสร็จ

๒.๑.๗ ปิดคอมพิวเตอร์เมื่อการใช้งานเสร็จสิ้น หรือเมื่อยุติการใช้งานเกินกว่า ๑ ชั่วโมง

๒.๒ การควบคุมทรัพย์สินสารสนเทศ และการใช้งานระบบคอมพิวเตอร์

๒.๒.๑ สำหรับห้อง Data Center

๒.๒.๑.๑ พื้นที่ต้องติดตั้งสัญญาณเตือนภัย เพื่อแจ้งเตือนเมื่อมีการบุกรุก

๒.๒.๑.๒ ทดสอบระบบป้องกันการบุกรุก เพื่อตรวจสอบว่าใช้งานได้ตามปกติ

๒.๒.๑.๓ บันทึกวันและเวลาเข้า-ออก พื้นที่

๒.๒.๑.๔ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่

๒.๒.๑.๕ ผู้มาเยือนต้องติดบัตรก่อนเข้าพื้นที่

๒.๓ การใช้งานเครื่องคอมพิวเตอร์ที่เป็นทรัพย์สินของหน่วยงาน

๒.๓.๑ การใช้งานทั่วไป

๒.๓.๑.๑ ผู้ใช้งานต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของหน่วยงาน

๒.๓.๑.๒ ติดตั้งโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย และห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว

๒.๓.๑.๓ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องตรวจสอบไวรัสก่อนใช้งาน

๒.๓.๒ การสำรองข้อมูลและการกู้คืน

๒.๓.๒.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลไว้บนสื่อบันทึกอื่น ๆ

๒.๓.๒.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาข้อมูล การสำรองข้อมูลให้เก็บไว้ในที่เหมาะสม

๒.๔ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-MAIL) การกำหนดสิทธิการเข้าถึง

๒.๔.๑ ผู้ที่ต้องการใช้งานต้องกรอกแบบฟอร์มเพื่อขอลงทะเบียน

๒.๔.๒ ผู้ใช้งานจะต้องรักษาชื่อผู้ใช้รหัสผ่านเป็นความลับ

๒.๔.๓ ห้ามเข้าถึง E-mail ของผู้อื่นเพื่ออ่าน หรือรับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอม จากเจ้าของ

๒.๔.๔ หลังการใช้งานให้ออกจากระบบทุกครั้ง

๒.๕ การใช้งานระบบอินเทอร์เน็ต

๒.๕.๑ การใช้งานเครื่องคอมพิวเตอร์ จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัส

๒.๕.๒ ไม่ใช้ระบบอินเทอร์เน็ตของกรมฝนหลวงและการบินเกษตร หาประโยชน์ในเชิงพาณิชย์

๒.๕.๓ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงาน

๒.๕.๔ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมละเมิดลิขสิทธิ์

๒.๕.๕ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น ที่ยั่วยุ หรือ ให้ร้าย

๒.๕.๖ ออกจากระบบเครือข่าย และปิดเว็บบราวเซอร์ทุกครั้งเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๓. มาตรการป้องกันด้านเทคนิค (Technical Safeguard)

๓.๑ มาตรการทำลายสื่อบันทึกข้อมูล/ข้อมูลอิเล็กทรอนิกส์

๓.๑.๑ สื่อบันทึกข้อมูลที่เป็นประเภทจานแม่เหล็กให้ทำการ Format หรือวิธีบดขยี้

๓.๑.๒ สื่อบันทึกข้อมูลประเภท Optical Disk ทำลาย โดยวิธีบดขยี้ หรือการหัก

๓.๑.๓ สื่อบันทึกข้อมูลขนาดเล็กแบบพกพา (Flash Drive) ให้ทำการ Format

๓.๑.๔ มีกระบวนการในการลบหรือเขียนข้อมูลทับบนข้อมูลก่อนเพื่อป้องกันการเข้าถึงข้อมูล เช่น การกู้ข้อมูล

๓.๑.๕ ผู้ใช้งานอาจนำการเข้ารหัส (Encryption) มาใช้กับข้อมูลที่เป็นความลับ

๓.๒ การควบคุมการเข้าถึงระบบปฏิบัติการระบบสารสนเทศ

๓.๒.๑ ผู้ดูแลระบบ ต้องติดตั้งโปรแกรมช่วยบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงาน หรือ Active Directory (กรมยังไม่มีการดำเนินงานส่วนนี้)

๓.๒.๒ การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตน

๓.๒.๓ ระบบสารสนเทศต้องมีการยืนยันตัวตนของผู้ใช้งาน

๓.๒.๔ การบริหารจัดการรหัสผ่าน โดยผู้ใช้งานต้องเปลี่ยนรหัสผ่านในครั้งแรกที่เข้าสู่ระบบ

๓.๒.๕ การควบคุมโปรแกรม ที่ผู้ใช้สามารถหลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้

๓.๒.๖ เมื่อไม่มีการใช้งานระบบสารสนเทศในระยะเวลาที่กำหนดให้ยุติการใช้งานระบบ ซึ่งกำหนดไว้ ๑๐ นาที (กรมยังไม่มีการดำเนินงานส่วนนี้ login แล้วใช้ไปได้ตลอด)

๓.๒.๗ การจำกัดระยะเวลาการเชื่อมต่อระบบเครือข่าย กำหนดได้ไม่เกินครั้งละ ๑๒ ช.ม.

๓.๓ การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ

๓.๓.๑ การจำกัดการเข้าถึงสารสนเทศ

๓.๓.๑.๑ กรณีมีการจ้างเหมาพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๓.๓.๑.๒ บริหารจัดการการเข้าถึงผู้ใช้งาน

๓.๓.๒ ระบบซึ่งไวต่อการรบกวนและมีความสำคัญสูงต่อหน่วยงาน

๓.๓.๒.๑ ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น เช่น ระบบฐานข้อมูลโรคของกรมฝนหลวงและการบินเกษตร

๓.๓.๒.๒ มีห้องปฏิบัติงานเป็นสัดส่วน และกำหนดสิทธิเฉพาะผู้มีสิทธิใช้งาน

๓.๓.๓ อุปกรณ์คอมพิวเตอร์และระบบการสื่อสาร

๓.๓.๓.๑ ผู้ใช้จึงต้องใช้งานอุปกรณ์อย่างมีประสิทธิภาพเพื่องานของกรมฝนหลวงและการบินเกษตร

๓.๓.๓.๒ โปรแกรมลิขสิทธิ์ของกรมฝนหลวงและการบินเกษตร ห้ามผู้ใช้นำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว

๓.๓.๓.๓ การปฏิบัติงานจากภายนอกหน่วยงาน ต้องดำเนินการตามมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของกรมฝนหลวงและการบินเกษตร

๓.๓.๓.๔ บุคคลภายนอกที่ต้องการเข้าใช้งานระบบสารสนเทศ ต้องเขียน แบบฟอร์มขออนุมัติจากผู้ดูแลหน่วยงาน

๓.๓.๓.๕ ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของกรมฝนหลวงและการบินเกษตร

๓.๔ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๓.๔.๑ ผู้ต้องการใช้งาน ต้องทำการลงทะเบียนกับผู้ดูแลระบบ

๓.๔.๒ ผู้ดูแลระบบเครือข่ายกรมฝนหลวงและการบินเกษตร ต้องดำเนินการดังต่อไปนี้

๓.๔.๒.๑ การวางอุปกรณ์กระจายสัญญาณในที่เหมาะสม เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเข้าใช้ระบบ

๓.๔.๒.๒ ตั้งค่าล็อกอินและรหัสผ่านการทำงานของอุปกรณ์ไร้ ที่สายคาดเดาได้ยาก

๓.๔.๒.๓ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๓.๔.๒.๔ ติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

๓.๔.๒.๕ ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

๓.๕ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ดังต่อไปนี้

๓.๕.๑ จัดเก็บข้อมูลระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ ข้อมูลที่จัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึง

๓.๕.๒ ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้

๓.๕.๓ กำหนดให้มีการเก็บบันทึกการทำงานของระบบ ไว้อย่างน้อย ๙๐ วัน

๓.๖ จำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เข้าถึงได้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๔. แนวปฏิบัติระบบสารสนเทศ และระบบสำรองของสารสนเทศหน่วยงานภายในกรมฝนหลวงและการบินเกษตร ต้องให้ผู้รับผิดชอบระบบสารสนเทศทุกระบบ จัดทำแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล โดยจัดระบบสำรองที่ เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๔.๑ การจัดทำบัญชีระบบสารสนเทศทั้งหมดของหน่วยงาน และการสำรองข้อมูลระบบสารสนเทศ

๔.๑.๑ กำหนดความถี่ในการสำรอง พร้อมบันทึก วัน/เวลา ชื่อข้อมูลที่สำรอง

๔.๑.๒ ตรวจสอบความครบถ้วนของการสำรองข้อมูลที่เกี่ยวข้อง เช่น คอนฟิกกูเรชัน และซอฟต์แวร์ร่วมต่าง ๆ

๔.๑.๓ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ กรณีเกิดความเสียหายกับอุปกรณ์สำรองหลัก

๔.๑.๔ จัดทำคู่มือขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล

๔.๑.๕ มีการทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ

๔.๒ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๔.๒.๑ กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้อง

๔.๒.๒ กำหนดขั้นตอนปฏิบัติในการสำรอง และทดสอบการกู้คืนระบบสารสนเทศ

๔.๒.๓ กำหนดเป็นแผนการสำรองระบบสารสนเทศ

๔.๒.๔ มีการทบทวนเพื่อปรับปรุงแผนให้สอดคล้องกับภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๕. แนวปฏิบัติการตรวจสอบ และประเมินความเสี่ยงด้านสารสนเทศ

๕.๑ จัดทำแผนบริหารความเสี่ยงด้านสารสนเทศของกรมฝนหลวงและการบินเกษตร เพื่อตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๕.๒ แนวทางในการตรวจสอบและประเมินความเสี่ยง

๖. การใช้งานเครือข่ายสังคมออนไลน์

๖.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ ตามที่กรมฝนหลวงและการบินเกษตรได้กำหนดไว้เท่านั้น

๖.๒ ผู้ใช้งานต้องตระหนักถึงความมั่นคงปลอดภัยในการใช้งาน และต้องรับผิดชอบหากเกิดความเสียหาย

๖.๓ ไม่อนุญาตให้ใช้งานเผยแพร่ข้อมูลที่เป็นความลับ และมีผลกระทบต่อบุคคลอื่น

๖.๔ ให้ใช้งานเครือข่ายสังคมออนไลน์ได้เท่าที่จำเป็นโดยไม่เบียดบังเวลาปฏิบัติงาน

๖.๕ หากเกิดปัญหาจากการใช้งาน ต้องแจ้งผู้ดูแลระบบโดยเร็วเพื่อดำเนินการตามความเหมาะสม

มาตรา ๓๗ (๒) *ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ*

ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน (Data Protection Officer) ตรวจสอบเบื้องต้น และแจ้งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของกรมทราบ

๑. การประเมินก่อนส่งมอบข้อมูล

๑.๑ ให้ดำเนินการตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคล และ/หรือ นิติบุคคลรายอื่นนั้นใช้เพื่อร้องขอข้อมูลส่วนบุคคล

๑.๒ ให้สอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด (เช่น จำเป็นต้องทราบวัน-เดือน-ปีเกิด หรือบ้านเลขที่ หรือไม่ หรือเพียงปี พ.ศ. เกิด และ รหัสไปรษณีย์ ก็เพียงพอ) และจำเป็นต้องทราบข้อมูลที่ชี้จำเพาะบุคคล (เช่น ชื่อ-นามสกุล เลข

ประจำตัว ๑๓ หลัก) หรือไม่ หากแปลงข้อมูลที่ชี้จำเพาะบุคคลแทนด้วยรหัสใหม่ที่เป็นนิรนามจะเพียงพอต่อการนำไปใช้ประโยชน์หรือไม่

๒. เมื่อส่งมอบข้อมูล

๒.๑ จัดเตรียมข้อมูลใหม่จากข้อมูลดิบให้มีระดับรายละเอียดเท่าที่จำเป็นต่อจุดประสงค์การใช้งาน

๒.๒ ส่งมอบข้อมูล พร้อมทำการบันทึกชื่อผู้ขอข้อมูล ข้อมูลสำหรับติดต่อ วัน-เดือน-ปี ที่ให้ข้อมูล ฐานกฎหมายที่ใช้สำหรับเข้าถึงข้อมูลส่วนบุคคล ตลอดจนวัตถุประสงค์การนำไปใช้งาน

๒.๓ แจ้งให้บุคคล หรือ นิติบุคคลนั้น ทราบว่าเมื่อรับข้อมูลไปแล้ว ผู้รับข้อมูลจะต้องดำเนินการตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลสำหรับข้อมูลชุดที่ร้องขอไปนั้นเช่นเดียวกัน ตามขอบเขตและวัตถุประสงค์การใช้งานที่แจ้งไว้

๓. หลังส่งมอบข้อมูล

๓.๑ ให้ติดตามการใช้งานเป็นครั้งคราวทุก ๓ เดือน ๖ เดือน หรือ ๑ ปี เพื่อบันทึกสถานะล่าสุดในการใช้งานข้อมูลนั้น หากไม่มีความจำเป็นใช้งานตามวัตถุประสงค์ที่แจ้งไว้เดิม ควรแจ้งให้บุคคล หรือ นิติบุคคลนั้นลบทำลายข้อมูล

๓.๒ กำหนดวิธีการในการปรับปรุงข้อมูลให้ทันสมัยต่อการใช้งานของผู้ใช้อยู่เสมอ เช่น มีโปรแกรมคอมพิวเตอร์สำหรับเชื่อมต่อปรับปรุงให้ข้อมูลต้นทางและปลายทางมีความทันสมัยเท่ากันโดยอัตโนมัติตลอดเวลา

มาตรา ๓๗ (๓) *จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามมาตรา ๒๔ (๑) หรือ (๔) หรือมาตรา ๒๖ (๕) (ก) หรือ (ข) การใช้เพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย ทั้งนี้ ให้นำความใน มาตรา ๓๓ วรรคห้า มาใช้บังคับกับการลบหรือทำลายข้อมูลส่วนบุคคลโดยอนุโลม*

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของหน่วยงาน(Data Protection Officer) ดำเนินการ และแจ้งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของกรมทราบ

๑. **ให้ติดตาม**ข้อมูลส่วนบุคคล**อย่างสม่ำเสมอ ทุกสัปดาห์ ทุกเดือน** ข้อมูลส่วนบุคคลนั้น มีรายการหรือ**มีชุดข้อมูลใดที่พ้นกำหนดระยะเวลาการเก็บรักษา**หรือไม่ (ตามที่แจ้งเจ้าของข้อมูลส่วนบุคคล (Data Subject) **ไว้ในประกาศความเป็นส่วนตัว (Privacy Notice)** หรือ ตามที่ขอความยินยอมไว้ (Consent Form) ทั้งนี้**เพื่อดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้** ตามแต่กรณี

๒. **กรณีเจ้าของข้อมูลส่วนบุคคลขอใช้สิทธิให้ลบทำลายข้อมูล** (หรือขอถอนความยินยอม) ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ควบคุมข้อมูลส่วนบุคคลใช้ฐานความยินยอมในการเก็บรวบรวมข้อมูลส่วนบุคคลเช่นนี้ **ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการลบทำลายหรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้** ตามแต่กรณี

๓. **การลบทำลายข้อมูล** หรือ การทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ **อาจยกเว้นไม่กระทำก็ได้ในกรณีผู้ควบคุมข้อมูลส่วนบุคคลมีเหตุผลความจำเป็นที่เหนือกว่าสิทธิของเจ้าของข้อมูล** เช่น

(ก) เพื่อวัตถุประสงค์การจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ การศึกษาวิจัยหรือสถิติ

(ข) เพื่อการสร้างประโยชน์สาธารณะตามหน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลรายนั้น

(ค) เพื่อประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

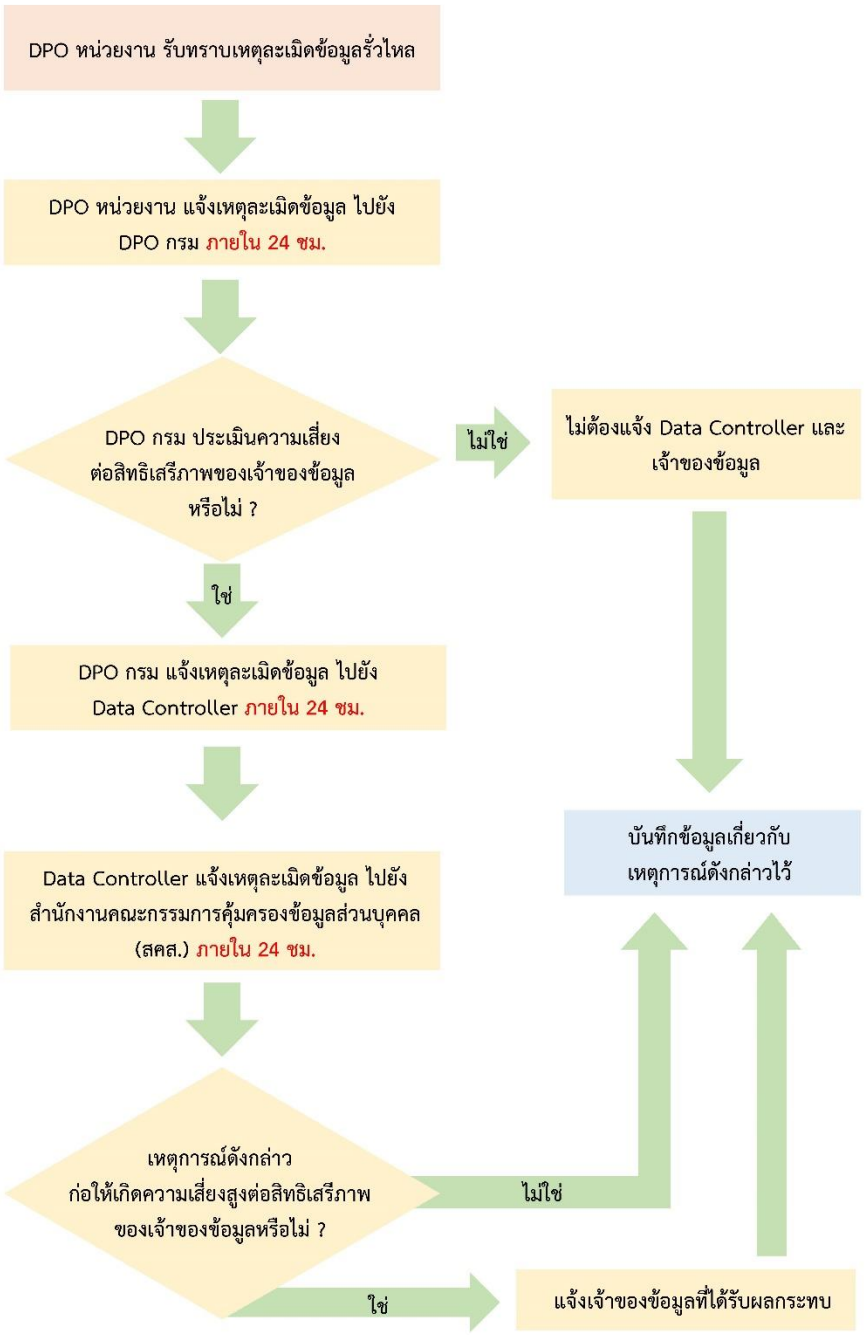
(ง) การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์

ทั้งนี้ ต้องจัดให้มีมาตรการดูแลข้อมูลที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

มาตรา ๓๗ (๔) *แจ้งเหตุการละเมิดข้อมูลส่วนบุคคลแก่สำนักงานโดยไม่ชักช้าภายในเจ็ดสิบสองชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้แจ้งเหตุการละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยาโดยไม่ชักช้าด้วย ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการประกาศกำหนด*

ให้ผู้เกี่ยวข้องแจ้งเหตุการละเมิด ตามผังกระบวนงานแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและวิธีการดังนี้

ขั้นตอนการดำเนินการ
กรณีที่มีการละเมิดข้อมูลส่วนบุคคล



กระบวนงานแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ภายใน ๗๒ ชั่วโมง

หมายเหตุ : DPO คือ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

๑. ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของหน่วยงานดำเนินการรับผิดชอบแจ้งเหตุละเมิดให้แก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของกรมทราบ ด้วยวิธีการ การส่งอีเมล์ หรือแจ้งช่องทางอิเล็กทรอนิกส์ และแจ้งทางโทรศัพท์กรณีเป็นเหตุละเมิดที่มีความรุนแรงและเร่งด่วน ภายใน ๒๔ ชั่วโมง

๒. ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของกรม แจ้งเหตุละเมิดให้แก่ผู้ควบคุมข้อมูล (Data Controller) ภายใน ๒๔ ชั่วโมง และผู้ควบคุมข้อมูล (Data Controller) ดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลได้ภายใน ๒๔ ชั่วโมง รวมเป็น ๗๒ ชั่วโมง (นับแต่ทราบเหตุ)

๓. **การแจ้งเหตุละเมิดอาจได้รับยกเว้นไม่ต้องดำเนินการก็ได้** หากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ตัวอย่างการประเมินความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่น

๓.๑ ตัวอย่างกรณีความเสี่ยงต่ำ: ข้อมูลส่วนบุคคลถูกเข้ารหัส (ไม่สามารถเปิดอ่านได้หากไม่ทราบรหัสผ่าน) ถูกซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เข้ารหัสจนไม่สามารถใช้งานได้ และไม่ได้ถูกโจรกรรมข้อมูลออกไป อย่างไรก็ตามผู้ควบคุมข้อมูลส่วนบุคคลมีระบบสำรองรองรับการบริการได้อย่างต่อเนื่อง กรณีนี้ถือได้ว่ามีความเสี่ยงต่ำที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

๓.๒ ตัวอย่างกรณีความเสี่ยงสูง: เว็บไซต์รับสมัครงานออนไลน์ถูกละเมิด โดยผู้โจมตีทำการฝังมัลแวร์เพื่อเข้าถึงข้อมูลใบสมัครงานออนไลน์(ตรวจพบ ๑ เดือนหลังมัลแวร์ถูกติดตั้ง) เนื้อหาข้อมูลเป็นข้อมูลทั่วไปเพื่อการสมัครงาน อย่างไรก็ตาม ถือว่ามีความเสี่ยงสูงที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่นนี้ ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการบันทึก (เป็นการภายใน) ว่าเคยมีเหตุโจรกรรม พร้อมทั้งแจ้งเหตุดังกล่าว (ภายใน ๗๒ ชั่วโมง) ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และยังต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบด้วย

๓.๓ ตัวอย่างกรณีความเสี่ยงต่ำ: เจ้าหน้าที่ของหน่วยงานส่งอีเมลล์ไปยังผู้รับผิดพลาด ซึ่งแนบไฟล์รายชื่อผู้เข้าอบรมหลักสูตรภาษาอังกฤษ ซึ่งประกอบไปด้วย ชื่อ-นามสกุล ที่อยู่อีเมลล์ และข้อจำกัดในการทานอาหาร ซึ่งมีเพียง ๒ คน ใน ๑๕ คนที่ระบุว่า แพ้น้ำตาลแลคโตสในนม (ถือเป็นข้อมูลสุขภาพ) กรณีนี้อีเมลล์ถูกส่งไปยังผู้เข้าอบรมในรุ่นก่อนหน้าแทนที่จะเป็นเจ้าหน้าที่ของโรงแรมที่จัดอาหาร ซึ่งถือเป็นการทำให้ข้อมูลส่วนบุคคลรั่วไหล อย่างไรก็ตามแม้ข้อมูลสุขภาพ จะถูกเผยแพร่ไปยังผู้ไม่เกี่ยวข้อง แต่ก็ไม่สามารถระบุความเสี่ยงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลได้แน่ชัด เช่นนี้ ถือว่าเป็นกรณีที่มีความเสี่ยงต่ำผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้ (เป็นการภายใน) ก็เพียงพอ ไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

มาตรา ๓๗ (๕) *ในกรณีที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลตามมาตรา ๕ วรรคสอง ต้องแต่งตั้งตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลเป็นหนังสือซึ่งตัวแทนต้องอยู่ในราชอาณาจักรและตัวแทนต้องได้รับมอบอำนาจให้กระทำการแทนผู้ควบคุมข้อมูลส่วนบุคคลโดยไม่มีข้อจำกัดความรับผิดใด ๆ ที่เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ของผู้ควบคุมข้อมูลส่วนบุคคล*

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลในข้อนี้ ยังไม่มีความจำเป็นที่ กรมฝนหลวงและการบินเกษตรต้องดำเนินการใด ๆ