แนวปฏิบัติการดำเนินงานด้านธรรมาภิบาลข้อมูล
(Data Governance Procedure)

จัดทำโดย
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงการท่องเที่ยวและกีฬา

๑. หลักการและขอบเขต

แนวปฏิบัติการบริหารจัดการข้อมูล (Data Management Guideline) ได้กำหนดขึ้นให้สอดคล้องตามนโยบายการบริหารจัดการข้อมูล (Data Management Policy) ที่สำนักงานปลัดกระทรวงการท่องเที่ยวและกีฬาประกาศ ซึ่งเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูลภาครัฐ จัดทำโดย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงการท่องเที่ยวและกีฬา มีผลบังคับใช้กับผู้มีส่วนได้เสียที่เกี่ยวข้องกับข้อมูลตามแนวปฏิบัติที่สำนักงานปลัดกระทรวงการท่องเที่ยวและกีฬา ประกาศ ซึ่งมีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามอย่างเคร่งครัด และผู้ใช้อื่นที่เกี่ยวข้องแต่ไม่มีหน้าที่ในการดูแลข้อมูลจะต้องให้ความร่วมมือในการดำเนินการตามแนวปฏิบัตินี้ ผู้ฝ่าฝืนมีความผิดและจะต้องได้รับการดำเนินการตามระเบียบของหน่วยงาน โดยแนวปฏิบัติจะต้องครอบคลุมกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูลและองค์ประกอบในการบริหารจัดการข้อมูล ดังรูป

ภาพที่ ๑ วงจรชีวิตของข้อมูล (Data Lifecycle)

๒. วงจรชีวิตของข้อมูล (Data Lifecycle)

๑. การสร้างข้อมูล (Create) เป็นการสร้างข้อมูลขึ้นมาใหม่ หรือปรับปรุงข้อมูลขึ้นใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการซื้อข้อมูล หรือการรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง

๒. การจัดเก็บข้อมูล (Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือข้อมูลที่ได้จากการเชื่อมโยงและ/หรือแลกเปลี่ยนกับหน่วยงานอื่น ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS) เพื่อให้เกิดความมีระเบียบง่ายต่อการใช้งาน ข้อมูลไม่สูญหายหรือถูกทำลาย และช่วยให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่าง รวดเร็ว

/๓. การประมวณ...

๓. การประมวลผลและใช้ข้อมูล (Processing and Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำ ข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอก ข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความ เสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูล กลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

๔. การเผยแพร่ข้อมูล (Disclosure) เป็นการนำข้อมูลที่อยู่ในความครอบครองของหน่วยงาน เผยแพร่ตามช่องทางต่าง ๆ อย่างเหมาะสม อาทิ การเปิดเผยข้อมูล (Open data) การแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่าง หน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition)

๕. กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการย้ายข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อเก็บรักษาถาวรโดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งาน ได้ใหม่เมื่อต้องการ

๖. การทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

๗. การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Linkage and Exchange) การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานทั้งภายในและภายนอกให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

๓. หมวดหมู่และการจัดระดับชั้นของข้อมูล

ข้อมูลขององค์กรสามารถแบ่งหมวดหมู่ตามกรอบธรรมาภิบาลข้อมูลและการใช้งานภายในสำนักงาน ดังนี้

๑) ข้อมูลความลับทางราชการ
๒) ข้อมูลส่วนบุคคล
๓) ข้อมูลองค์กร
๔) ข้อมูลสาธารณะ
๕) ข้อมูลใช้ภายในหน่วยงาน

ภาพที่ ๒ หมวดหมู่ข้อมูล

/โดยมีการ...

โดยมีการจัดระดับชั้นความลับของข้อมูล ดังนี้

ภาพที่ ๓ ระดับชั้นข้อมูล

๑) ข้อมูลใช้ภายใน (Internal Use) ได้แก่ ข้อมูลสำหรับใช้ในการดาเนินกิจการภายในของหน่วยงาน ซึ่งไม่อนุญาตให้นาไปใช้งานภายนอกก่อนได้รับอนุญาต ได้แก่ นโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงาน เป็นต้น

๒) ข้อมูลที่มีชั้นความลับ (Secret) แบ่งเป็น ๓ ระดับ ได้แก่ ข้อมูลลับที่สุด (Top Secret) ข้อมูลลับมาก (Secret) และข้อมูลลับ (Confidential)

๓) ข้อมูลเปิดเผยได้ (Public) ได้แก่ ข้อมูลที่สามารถเปิดเผยบุคคลทั่วไป โดยไม่ก่อให้เกิดความเสียหายใด ๆ แก่สำนักงาน ได้แก่ ข้อมูลเผยแพร่บนเว็บไซต์ ข้อมูลจากการแถลงข่าว หรือรายงานประจำปีของสำนักงาน เป็นต้น

๔. ผู้มีส่วนได้เสีย (Stakeholders)

ตามแนวปฏิบัติการบริหารจัดการข้อมูลนี้ บังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง กับข้อมูลตามประกาศแนวปฏิบัติการบริหารจัดการข้อมูลของสำนักงาน รวมถึงผู้เกี่ยวข้องอื่น ๆ ที่ไม่ได้ระบุไว้ในแนวปฏิบัติ ดังนี้

1) ผู้สร้างข้อมูล (Data Creators)
2) ผู้ใช้ข้อมูล (Data Users)
3) เจ้าของข้อมูล (Data Owners)
4) บริกรข้อมูล (Data Stewards)
5) ผู้ดูแลระบบสารสนเทศ (System Administrators)
6) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)
7) ผู้ทำลายข้อมูล (Data Disposers)
8) เจ้าของข้อมูลส่วนบุคคล (Data Subjects)
9) ผู้จัดการโครงการ (Project Managers)
10) ผู้ดูแลระบบแม่ข่าย (Server Administrators)

/๕. คำนิยาม...

๕. คำนิยาม

ในแนวปฏิบัติฯ ฉบับนี้

(๑) **สำนักงาน** หมายความว่า สำนักงานปลัดกระทรวงการท่องเที่ยวและกีฬา

(๒) **ผู้บริหารระดับสูง** หมายความว่า ปลัดกระทรวงการท่องเที่ยวและกีฬา

(๓) **ผู้บริหาร** หมายความว่า ผู้บริหารตั้งแต่ระดับผู้อำนวยการสำนัก/สถาบัน/กอง/กลุ่ม

(๔) **บุคลากร** หมายความว่า บุคลากรของสำนักงาน

(๕) **เจ้าหน้าที่** หมายความว่า บุคคลหรือลูกจ้างที่มีสัญญาจ้างให้ปฏิบัติงาน เป็นการชั่วคราวและมีกำหนดระยะเวลาและสิ้นสุดที่แน่นอน

(๖) **ผู้บังคับบัญชา** หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงาน

(๗) **ผู้สร้างข้อมูล (Data Creators)** หมายความว่า เจ้าหน้าที่ทุกสำนักและฝ่ายที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ รวมถึงทำงานร่วมกับบริกรข้อมูล เพื่อ ตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความปลอดภัยของข้อมูล

(๘) **ผู้ใช้งาน (Users)** หมายความว่า บุคคลที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามา ใช้งาน บริหาร หรือดูแลรักษาระบบสารสนเทศของสำนักงาน ตามสิทธิ์และหน้าที่ความรับผิดชอบ

(๙) **ผู้ใช้ข้อมูล (Data Users)** หมายความว่า บุคลากรที่นำข้อมูลไปใช้งานทั้งในระดับบริหาร และ ระดับปฏิบัติงานสิทธิ์ของผู้ใช้งาน หมายความว่า สิทธิ์และหน้าที่ตามบทบาท (Role) ที่เกี่ยวข้องกับระบบสารสนเทศ ของสำนักงาน มีดังนี้

- ๑) **สิทธิ์ใช้งานทั่วไป** หมายถึง คณะกรรมการ ผู้อำนวยการ เจ้าหน้าที่ ลูกจ้าง นิสิตและนักศึกษาฝึกงานทั้งหมดที่ใช้งานระบบสารสนเทศพื้นฐานของสำนักงาน ผู้ใช้งานต้องขออนุญาตจากผู้อำนวยการสำนัก/ ผู้อำนวยการฝ่ายขึ้นไป โดยให้ใช้แบบฟอร์มเพื่อขออนุมัติตามที่สำนักงานกำหนด
- ๒) **สิทธิ์จำเพาะ** หมายถึง สิทธิ์เฉพาะตามหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการปฏิบัติงาน ผู้ใช้งานต้องได้รับสิทธิ์จากผู้บังคับบัญชา
- ๓) **สิทธิ์พิเศษ** หมายถึง สิทธิ์ที่ได้รับมอบหมายเพิ่มเติมจากผู้บังคับบัญชาเป็นกรณีพิเศษ ผู้ใช้งานต้องได้รับมอบหมายจากผู้บังคับบัญชาเป็นครั้งคราว

(๑๐) **เจ้าของข้อมูล (Data Owners)** หมายความว่า ผู้ที่รับผิดชอบข้อมูลของสำนักงาน โดยเจ้าของข้อมูลเป็นผู้ที่รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย ดังต่อไปนี้

- ๑) รองอธิบดีสำนักงาน ที่กำกับดูแล ในกรณีที่ข้อมูลนั้นไม่อยู่ในความรับผิดชอบของผู้อำนวยการหน่วยงาน
- ๒) ผู้อำนวยการหน่วยงาน (สำนัก/สถาบัน/กอง/กลุ่ม)

(๑๑) **เจ้าของระบบงาน (System Owner)** หมายความว่า ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแล และบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในสำนักงาน

(๑๒) **เจ้าของข้อมูลส่วนบุคคล (Data Subjects)** หมายความว่า เจ้าหน้าที่ที่เป็นเจ้าของข้อมูล ส่วนบุคคลนั้น

(๑๓) **บริกรข้อมูล (Data Stewards)** หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ ตามแนวทางการกำกับดูแลข้อมูล กำกับ/ตรวจสอบผู้มีส่วนได้ส่วนเสียกับข้อมูลปฏิบัติตามนโยบายและ แนวปฏิบัติการดำเนินงานด้านธรรมาภิบาลข้อมูล

/(๑๔) ผู้ดูแลระบบ...

(๑๔) **ผู้ดูแลระบบสารสนเทศ (System Administrators)** หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมาย จากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

(๑๕) **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)** หมายความว่า ผู้บริหารที่ได้รับการแต่งตั้งจากสำนักงาน ให้ปฏิบัติหน้าที่เป็นผู้ควบคุมข้อมูลส่วนบุคคลของสำนักงาน

(๑๖) **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)** หมายความว่า ผู้บริหาร หรือเจ้าหน้าที่ที่ ได้รับมอบหมายปฏิบัติหน้าที่เป็นบริกรข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เพื่อประมวลผลข้อมูลส่วนบุคคล ของสำนักงาน

(๑๗) **หน่วยงานภายนอก/ผู้ให้บริการภายนอก/บุคคลภายนอก** หมายความว่า ผู้ประกอบการหรือ ผู้ให้บริการภายนอก (Third Party) ที่ยื่นคำขออนุญาตต่าง ๆ ผู้ดำเนินกิจการของผู้รับอนุญาต ผู้มีหน้าที่ปฏิบัติการ ผู้ร้องเรียนเรื่องราวต่าง ๆ ที่เกี่ยวข้องกับการทำงานของสำนักงาน โดยบุคคลภายนอกจะใช้ระบบสารสนเทศที่สำนักงาน เตรียมไว้ให้บริการสำหรับบุคคลภายนอก

(๑๘) **ข้อมูล (Data)** หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่า การสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วย ธุรกรรมอิเล็กทรอนิกส์

(๑๙) **สารสนเทศ (Information)** หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถ เข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

(๒๐) **ระบบคอมพิวเตอร์** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ ประมวลผลข้อมูลโดยอัตโนมัติ

(๒๑) **ข้อมูลดิจิทัล (Digital Data)** หมายความว่า ข้อมูลที่ได้จัดทำ จัดเก็บ จำแนกหมวดหมู่ ประมวลผล ใช้ ปกปิด เปิดเผย ตรวจสอบ ทำลาย ด้วยเครื่องมือหรือวิธีการทางเทคโนโลยีดิจิทัล

(๒๒) **ชุดข้อมูล (Dataset)** หมายความว่า การนำข้อมูลจากหลายแหล่งมารวม เพื่อจัดเป็นชุดให้ ตรงตามลักษณะโครงสร้างของข้อมูล

(๒๓) **คำอธิบายชุดข้อมูล (Metadata)** หมายความว่า ข้อมูลที่ใช้กำกับและอธิบาย ข้อมูลหลักหรือ กลุ่มของข้อมูลอื่น

(๒๔) **บัญชีชุดข้อมูล (Data Catalog)** หมายความว่า เอกสารรายการของชุดข้อมูลที่สำนักงาน ถือครอง หรือบริหารจัดการ

(๒๕) **ข้อมูลความลับทางราชการ** หมายความว่า ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของสำนักงาน ที่มีคำสั่งของรัฐไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับ

(๒๖) **ข้อมูลส่วนบุคคล (Personal Data)** หมายความว่า ข้อมูลที่เกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อมที่สำนักงาน เก็บและใช้

(๒๗) **ข้อมูลสาธารณะ (Public Data)** หมายความว่า ข้อมูลที่สามารถเปิดเผยแก่บุคคลทั่วไปได้ โดย ไม่ก่อให้เกิดความเสียหายใดๆ แก่สำนักงาน ได้แก่ ข้อมูลเผยแพร่บนเว็บไซต์ ข้อมูลจากการแถลงข่าว หรือรายงาน ประจำปีของสำนักงาน เป็นต้น

/(๒๘) ข้อมูลสำนักงาน...

(๒๘) **ข้อมูลสำนักงาน** หมายความว่า ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของสำนักงาน

(๒๙) **ข้อมูลจราจรทางคอมพิวเตอร์** หมายความว่าข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบ คอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิดต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของ บริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

(๓๐) **ข้อมูลลับที่สุด (Top Secret)** หมายความว่า ข้อมูลที่มีความสำคัญต่อสำนักงาน ในระดับสูงที่สุด หาก สูญหายหรือถูกเปิดเผย โดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อสำนักงาน ในระดับร้ายแรงที่สุด

(๓๑) **ข้อมูลลับมาก (Secret)** หมายความว่า ข้อมูลที่มีความสำคัญต่อสำนักงาน ในระดับสูงมาก หาก สูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อสำนักงาน ในระดับร้ายแรงมาก

(๓๒) **ข้อมูลลับ (Confidential)** หมายความว่า ข้อมูลที่มีความสำคัญต่อสำนักงาน ในระดับสูง หาก สูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาตจะส่งผลเสียหายต่อสำนักงาน

(๓๓) **ข้อมูลใช้ภายใน (Internal Use Only)** หมายความว่า ข้อมูล ข่าวสารที่ใช้ภายในสำนักงาน เท่านั้น

๕. การเผยแพร่และการทบทวน

แนวปฏิบัติการดำเนินงานด้านธรรมาภิบาลข้อมูลนี้จะต้องทำการเผยแพร่ สื่อสาร โดยการประกาศแจ้งเวียนในระบบอินทราเน็ตและจดหมายอิเล็กทรอนิกส์ รวมถึงการจัดอบรม/สัมมนาเพื่อให้เจ้าหน้าที่ทุกระดับในสำนักงาน ได้รับทราบ และถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด ซึ่งแนวปฏิบัตินี้จะต้องถูกทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ รวมถึงเมื่อมีข้อเสนอแนะจากคณะกรรมการข้อมูลข่าวสารและเปิดเผยข้อมูลภาครัฐ ในรูปแบบดิจิทัลของสำนักงาน

แนวปฏิบัติการบริหารจัดการข้อมูลสำนักงานปลัดกระทรวงการท่องเที่ยวและกีฬา

หมวด ๑ การสร้างข้อมูล

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการสร้างข้อมูลให้มีคุณภาพ มีความมั่นคงปลอดภัยและเป็นประโยชน์ต่อผู้ใช้ข้อมูล

ผู้มีส่วนได้เสีย

๑) เจ้าของข้อมูล (Data Owners)
๒) ผู้สร้างข้อมูล (Data Creators)
๓) บริกรข้อมูล (Data Stewards)
๔) ผู้ดูแลระบบสารสนเทศ (System Administrators)

อ้างอิง

๑.ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓
๒. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐
๓. พระราชบัญญัติลิขสิทธิ์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๘
๔. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๕. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. ๒๕๖๓
๖. ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑: ๒๐๑๓

/แนวปฏิบัติ...

แนวปฏิบัติ

๑. เจ้าของข้อมูล (Data Owners) เป็นผู้กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล และจะต้องทบทวนสิทธิ์นั้น อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

๒. เจ้าของข้อมูล (Data Owners) เป็นผู้กำหนดชั้นความลับของข้อมูลที่ถูกสร้างขึ้น ตามวิธีปฏิบัติการจำแนกชั้นความลับของข้อมูล

๓. กำหนดให้มีวิธีปฏิบัติการจำแนกชั้นความลับของข้อมูลสำหรับข้อมูลที่ถูกสร้างขึ้น

๔. ผู้ดูแลระบบสารสนเทศ (System Administrators) จะต้องกำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูล (Data Creators) ตามที่เจ้าของข้อมูล (Data Owners) กำหนด

๕. เจ้าของข้อมูล (Data Owners) และบริกรข้อมูล (Data Stewards) ร่วมจัดทำคำอธิบายชุดข้อมูล ดิจิทัล (Metadata) หรือ เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานขั้นต่ำ คำอธิบายชุดข้อมูลดิจิทัลที่สำนักงานกำหนด และกำหนดให้ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมินคุณค่าชุดข้อมูล ที่ สพร. หรือสำนักงาน กำหนด และเผยแพร่เป็นข้อมูลเปิด (Open data) ของหน่วยงานต่อสาธารณะ ตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล (Digital Data)

๖. ห้ามมิให้ผู้สร้างข้อมูล (Data Creators) นำข้อมูลที่มีลักษณะดังต่อไปนี้เข้าสู่ระบบคอมพิวเตอร์ที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

(๑) ข้อมูลที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน

(๒) ข้อมูลอันเป็นเท็จที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือโครงสร้างพื้นฐาน หรือก่อให้เกิดวามตื่นตระหนัก

(๓) ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือความผิดเกี่ยวกับการก่อการร้าย

(๔) ข้อมูลที่มีลักษณะอันลามก และคนทั่วไปอาจเข้าถึงได้

(๕) ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย

๗. ห้ามมิให้ผู้สร้างข้อมูล (Data Creators) ทำการสร้าง/ทำซ้ำต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่นเว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง

๘. กำหนดให้ผู้สร้างข้อมูล (Data Creators) สร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น

๙. เจ้าของข้อมูล (Data Owners) และบริกรข้อมูล (Data Stewards) ต้องตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น

๑๐. กำหนดให้มีวิธีปฏิบัติเกี่ยวกับสร้างข้อมูลให้มีความปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

/ภาพที่ ๔...

ภาพที่ ๔ แนวปฏิบัติ การสร้างข้อมูล

ตารางที่ ๑ แนวปฏิบัติในการสร้างข้อมูล

กิจกรรม	ผู้มีส่วนได้เสีย			
	ผู้สร้างข้อมูล	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล		X		
กำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูล				X
สร้างข้อมูลที่ไม่ขัดต่อกฎหมายและจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น	X			
กำหนดชั้นความลับข้อมูลของข้อมูลที่ถูกสร้างขึ้น		X		
จัดทำคำอธิบายชุดข้อมูลดิจิทัล		X	X	
ประเมินคุณค่าของชุดข้อมูลดิจิทัล		X		
ตรวจสอบความถูกต้องของข้อมูล		X		

หมวด ๒ การจัดเก็บข้อมูล

การจัดเก็บข้อมูล เป็นการจัดเก็บข้อมูลที่ได้จากกระบวนการสร้าง หรือกระบวนการเชื่อมโยงและแลกเปลี่ยนข้อมูลกับหน่วยงานอื่น เพื่อให้เกิดความมีระเบียบ ง่ายต่อการใช้งาน ข้อมูลไม่สูญหายหรือถูกทำลาย และช่วยให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการจัดเก็บข้อมูล ให้มีคุณภาพ เข้าถึงและใช้งานได้อย่างมั่นคงปลอดภัย

/ผู้มีส่วนได้เสีย...

ผู้มีส่วนได้เสีย

๑) เจ้าของข้อมูล (Data Owners)

๒) ผู้สร้างข้อมูล (Data Creators)

๓) ผู้ใช้ข้อมูล (Data Users)

๔) บริกรข้อมูล (Data Stewards)

๕) ผู้ดูแลระบบสารสนเทศ (System Administrators)

อ้างอิง

๑. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๓. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

๔. ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑: ๒๐๑๓

แนวปฏิบัติในการจัดเก็บข้อมูลทั่วไป

ภาพที่ ๕ แนวปฏิบัติการจัดเก็บข้อมูลทั่วไป

๑. กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูล และบริกรข้อมูล ร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน

๒. กำหนดให้เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน

๓. กำหนดให้บริกรข้อมูล และผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้ว เพื่อจัดเก็บเป็นข้อมูลถาวร

๔. ผู้มีส่วนได้ส่วนเสียเกี่ยวกับข้อมูล ทั้งเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และบริกรข้อมูลจะต้องจัดเก็บข้อมูลตามการจัดชั้นความลับของสำนักงาน

/๕. กำหนดให้...

๕. กำหนดให้ผู้มีส่วนได้ส่วนเสียเกี่ยวกับข้อมูล ทั้งเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และบริกรข้อมูล จัดเก็บข้อมูลที่มีชั้นความลับโดยทำการเข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้ การเข้ารหัสข้อมูลให้ปฏิบัติตามวิธีการเข้ารหัสข้อมูลแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน สำหรับกรณีที่ในตารางฐานข้อมูลเดียวกันมีฟิลด์ข้อมูลที่มีชั้นความลับและไม่มีชั้นความลับอยู่ร่วมกันให้ทำการเข้ารหัสข้อมูลเฉพาะฟิลด์ข้อมูลที่มีชั้นความลับเท่านั้น สำหรับกรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บดังนี้

(๑) เก็บในสถานที่เหมาะสม สามารถปิดล็อกได้เมื่อไม่ใช้งาน

(๒) เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ ได้แก่ เครื่องพิมพ์ เครื่องถ่ายเอกสาร เป็นต้น โดยทันที เพื่อเป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิ์ในการเข้าถึงข้อมูล เข้าถึงข้อมูลได้

แนวปฏิบัติการจัดเก็บข้อมูลส่วนบุคคล

ภาพที่ ๖ แนวปฏิบัติการจัดเก็บข้อมูลส่วนบุคคล

๖. กำหนดให้มีการจัดเก็บข้อมูลส่วนบุคคล โดยให้เก็บรวบรวมได้เท่าที่จาเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และไม่เก็บรวบรวมข้อมูลส่วนบุคคล ดังต่อไปนี้ เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูล

(๑) เชื้อชาติ

(๒) เผ่าพันธุ์

(๓) ความคิดเห็นทางการเมือง

(๔) ความเชื่อในลัทธิ ศาสนาหรือปรัชญา

(๕) พฤติกรรมทางเพศ

(๖) ประวัติอาชญากรรม

(๗) ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต

(๘) ข้อมูลสหภาพแรงงาน

(๙) ข้อมูลพันธุกรรม

(๑๐) ข้อมูลชีวภาพ

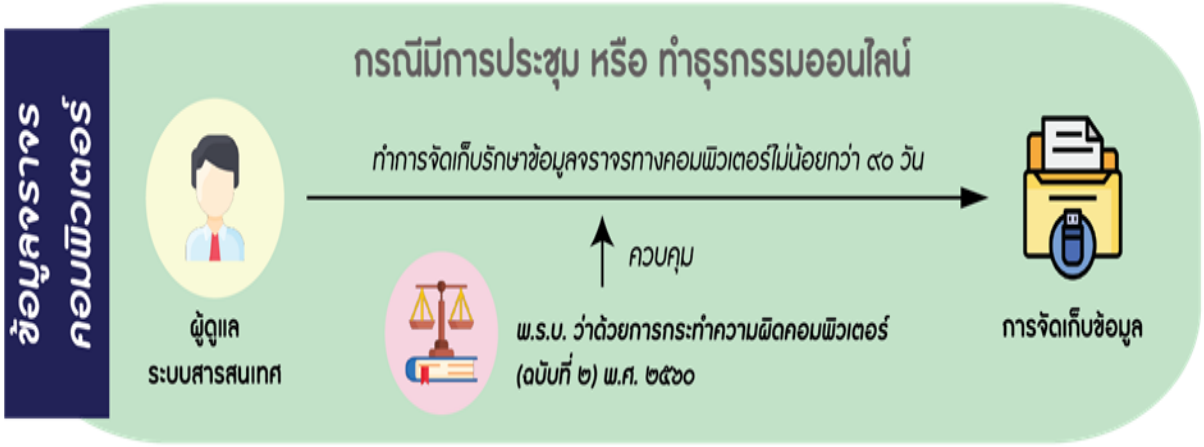
(๑๑) ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่หน่วยงานกำหนด

/๗. กำหนดให้...

๗. กำหนดให้การยกเลิกการจัดเก็บข้อมูลกรณีเจ้าของข้อมูลถอนความยินยอม ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

๘. กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

แนวปฏิบัติในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์



ภาพที่ ๗ แนวปฏิบัติในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์

๙. กำหนดให้การจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้

(๑) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง (Integrity) และระบุตัวตน(Identification) ที่เข้าถึงสื่อดังกล่าวได้

(๒) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับใน การเข้าถึง

(๓) ข้อมูลดังกล่าวเพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบแม่ข่ายแก้ไข ข้อมูลที่จัดเก็บไว้ได้

(๔) การจัดเก็บข้อมูลต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้ (Identification and Authentication)

๑๐. กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้ง กรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนาข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน

๑๑. กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บถาวร เพื่อป้องกันข้อมูลไม่ให้มีการลบ ปรับปรุง แก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บถาวรรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต

๑๒. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

๑๓. ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของหน่วยงานสำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่หน่วยงานจัดสรรไว้

/ตารางที่ ๒....

ตารางที่ ๒ แนวปฏิบัติในการจัดเก็บข้อมูล

กิจกรรม	ผู้มีส่วนได้เสีย				
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้สร้างข้อมูล	ผู้ใช้ข้อมูล	บริกรข้อมูล
กำหนดระยะเวลาในการจัดเก็บข้อมูล	x				
จัดเก็บข้อมูลตามการจัดชั้นความลับของสำนักงาน	x		x	x	x
จัดเก็บข้อมูลที่มีชั้นความลับโดยทำการเข้ารหัสข้อมูล	x		x	x	x
จัดเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น		x			
ยกเลิกการจัดเก็บข้อมูลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม		x			
จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์		x			
ทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดเพื่อจัดเก็บเป็นข้อมูลถาวร		x			

หมวด ๓ การประมวลผลข้อมูลและการใช้ข้อมูล

การประมวลผลและการใช้ข้อมูล เป็นการนาข้อมูลที่ได้จากการจัดเก็บมาประมวลผล ได้แก่การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล แสดงผลในรูปแบบตามวัตถุประสงค์ที่กำหนดเพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ที่จาเป็น

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติในการประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพถูกต้องตามวัตถุประสงค์ เพื่อให้เกิดประโยชน์สูงสุด

ผู้มีส่วนได้เสีย

๑) เจ้าของข้อมูล (Data Owners)
๒) ผู้ใช้ข้อมูล (Data Users)
๓) ผู้ทำลายข้อมูล (Data Disposers)
๔) ผู้ดูแลระบบสารสนเทศ (Systems Administrators)
๕) บริกรข้อมูล (Data Stewards)
๖) เจ้าของข้อมูลส่วนบุคคล (Data Subjects)

/อ้างอิง...

อ้างอิง

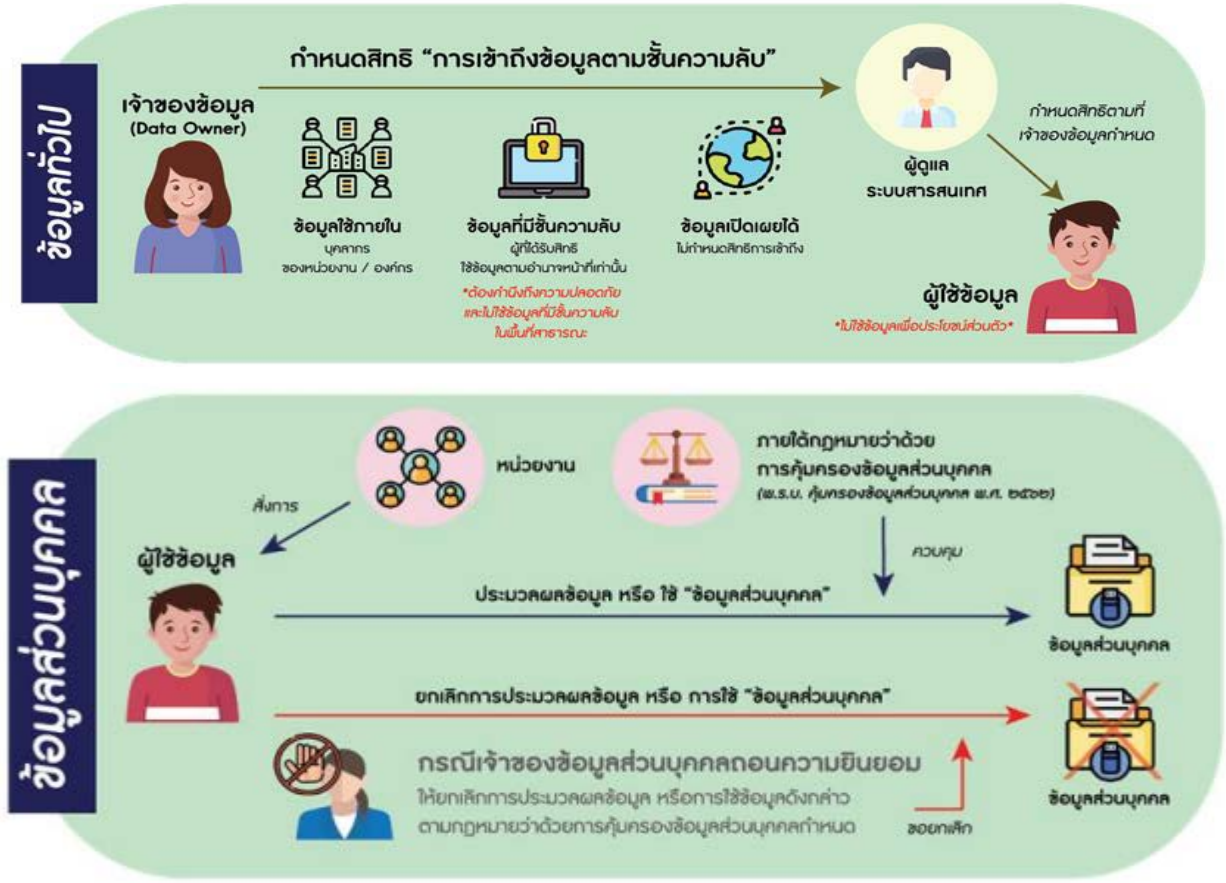
๑. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒. ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑: ๒๐๑๓

๓. พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. ๒๕๔๐

๔. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

แนวปฏิบัติ



ภาพที่ ๗ แนวปฏิบัติการประมวลผลและใช้ข้อมูล

๑. เจ้าของข้อมูล (Data Owners) และบริกรข้อมูล (Data Stewards) จัดทำคำอธิบายชุดข้อมูล (Metadata) สำหรับทุกชุดข้อมูลที่สามารถใช้งานได้ตามวัตถุประสงค์ของสำนักงาน

๒. เจ้าของข้อมูล (Data Owners) กำหนดผู้มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้ข้อมูล ตามชั้นความลับดังนี้

(๑) **ข้อมูลที่มีชั้นความลับ** กำหนดให้ผู้ใช้งานที่ได้รับสิทธิ์ตามตำแหน่ง/บทบาทเท่านั้น ทั้งนี้ ผู้ใช้งานที่ได้รับสิทธิ์จะต้องไม่ใช้ข้อมูลจริงในการใช้งาน และประมวลผล

(๒) **ข้อมูลใช้ภายใน** กำหนดให้ผู้บริหาร เจ้าหน้าที่ และลูกจ้างเท่านั้น ที่มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้ ทั้งนี้ ต้องปกป้องข้อมูลจากการเข้าถึงโดยบุคคลภายนอก

/(๓) ข้อมูลเปิด...

(๓) **ข้อมูลเปิดเผยได้** ไม่กำหนดสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล

๓. เจ้าของข้อมูล (Data Owners) จะต้องทบทวนสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ

๔. ผู้ดูแลระบบสารสนเทศ (System Administrators) จะต้องกำหนดสิทธิ์ในการเข้าถึงเพื่อประมวลผลและใช้ข้อมูลผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด และจัดทำระบบสำหรับการบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log Files) ของผู้ใช้ข้อมูล (Data User)

๕. ผู้ขอใช้หรือผู้ประมวลผลข้อมูล ต้องดำเนินการดังนี้

(๑) ขออนุมัติการใช้จากเจ้าของข้อมูล (Data Owners) โดยระบุขอบเขตและรายละเอียดของข้อมูลที่ร้องขอ เช่น วัตถุประสงค์ ความถี่ ระยะเวลาที่ต้องใช้

(๒) ต้องประมวลผลและใช้ข้อมูล ตามวัตถุประสงค์ที่แจ้งไว้กับจากเจ้าของข้อมูล (Data Owners) เท่านั้น

๖. การร้องขอข้อมูล ครอบคลุมการร้องขอข้อมูลในกรณีที่บุคคลหรือหน่วยงานภายนอก หน่วยงานภายใน ผู้ร้องเป็นบุคคลภายในหรือหน่วยงานภาครัฐโดยสิทธิ และเจ้าของข้อมูลในการปรับปรุงข้อมูล Metadata และดำเนินการตามร้องขอ ในกรณีที่บุคคล หรือหน่วยงานภายนอก ต้องการร้องขอข้อมูลของหน่วยงานในสำนักงาน ให้มีหนังสือเป็นลายลักษณ์อักษร สามารถพิจารณาได้ดังนี้

(๑) หากเป็นข้อมูลของผู้ร้องขอซึ่งเป็นเจ้าของข้อมูลโดยตรง ให้มีการยืนยันตัวตนก่อน โดยหน่วยงานที่เกี่ยวข้องต้องมีพิจารณาตรวจสอบและเร่งดำเนินการแก้ไขปรับปรุงข้อมูลนั้น

(๒) หากเป็นหน่วยงานภายนอก ทั้งรัฐหรือเอกชน หรือบุคคลอื่นที่ไม่ใช่เจ้าของข้อมูล ให้ดำเนินการตามคำสั่ง ระเบียบ และข้อกฎหมายใด ๆ ที่สำนักงาน กำหนด

๗. ผู้ใช้ข้อมูลจะประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล

๘. หน่วยงานต้องยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอม ตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

ตารางที่ ๓ แนวปฏิบัติในการประมวลผลและใช้ข้อมูล

กิจกรรม	ผู้มีส่วนได้เสีย			
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้ใช้ข้อมูล	บริกรข้อมูล
กำหนดผู้มีสิทธิ์ประมวลผลและเข้าใช้งานข้อมูลตามชั้นความลับ	x			
กำหนดสิทธิ์ในการประมวลผลและเข้าใช้งานข้อมูลให้แก่ผู้ใช้ข้อมูล		x		x
ไม่ใช้ข้อมูลในเครือข่ายของสำนักงาน เพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว			x	

/หมวด ๔...

หมวด ๔ การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

การเชื่อมโยงและแลกเปลี่ยนข้อมูล เป็นการนำข้อมูลสำนักงาน แลกเปลี่ยนทั้งระหว่างหน่วยงานภายในและภายนอกให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลทั้งภายในหน่วยงานและระหว่างหน่วยงานอย่างมีประสิทธิภาพ และก่อให้เกิดประโยชน์ต่อภาคประชาชนภาครัฐและภาคเอกชน

ผู้มีส่วนได้เสีย

- ผู้จัดการโครงการ (Project Managers)
- ผู้ดูแลระบบแม่ข่าย (Server Administrators)
- เจ้าของข้อมูล (Data Owners)
- บริกรข้อมูล (Data Stewards)

อ้างอิง

๑. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

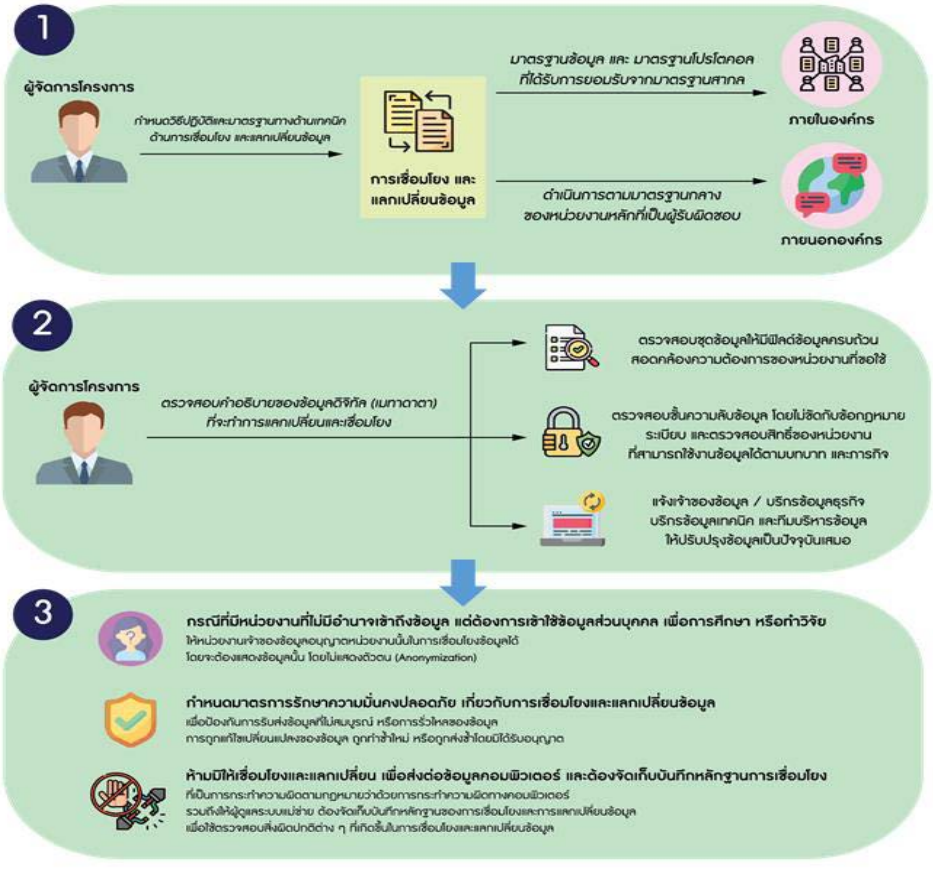
๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๔. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

๕. ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑: ๒๐๑๓

แนวปฏิบัติ



ภาพที่ ๘ แนวปฏิบัติ การเชื่อมโยงและแลกเปลี่ยนข้อมูล

๑. กำหนดให้เจ้าของข้อมูล หรือบริกรข้อมูลตามที่ได้รับมอบหมายดาเนินการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัล (ของข้อมูลที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้

(๑) ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้

(๒) ตรวจสอบชั้นความลับของข้อมูล ว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ นั่นคือต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับ ทางราชการ และความเป็นส่วนบุคคล พร้อมทั้ง ตรวจสอบสิทธิ์ของหน่วยงานที่สามารถนาข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ หากไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล และบริกรข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

๒. กำหนดให้เจ้าของข้อมูล หรือบริกรข้อมูลจัดทำแนวทางการทำงานร่วมกันในการเชื่อมโยงแลกเปลี่ยนข้อมูลทั้งระหว่างหน่วยงานภายในและหน่วยงานภายนอกของโครงการในความรับผิดชอบ โดยมีองค์ประกอบ ดังต่อไปนี้เป็นอย่างน้อย

(๑) วัตถุประสงค์ในการนำข้อมูลไปใช้งาน

(๒) ขอบเขตการนำข้อมูลไปใช้งาน

(๓) ช่วงเวลาและความถี่ในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้

(๔) ระดับการให้บริการ (Service Level Agreement: SLA)

(๕) ฟิลด์ข้อมูลที่สามารถเข้าถึง

(๖) รายการข้อมูลที่สามารถเข้าถึง ในกรณีขอข้อมูลส่วนบุคคลเป็นรายคน ต้องจัดทำหนังสือแสดงความยินยอม (Consent Letter) เพื่อรับการยินยอมจากบุคคลนั้น ๆ ยกเว้นหน่วยงานที่ขอใช้ข้อมูลมีอำนาจตามกฎหมายโดยชอบธรรม

(๗) กำหนดรายละเอียดหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล

(๘) กำหนดวิธียืนยันตัวตนในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

๓. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต

๔. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

๕. กำหนดให้ผู้ดูระบบสารสนเทศต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยง และการแลกเปลี่ยนข้อมูลดิจิทัล เพื่อใช้ตรวจสอบสิ่งผิดปกติต่าง ๆ ที่เกิดขึ้นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

๖. กำหนดให้มีวิธีปฏิบัติหรือระเบียบในการดาเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลระหว่างหน่วยงานของรัฐแห่งอื่นที่ได้จัดทำหรือรวบรวมข้อมูลดิจิทัลไว้เป็นข้อมูลหลักไม่ว่าทั้งหมด หรือบางส่วนโดยสำนักงาน ไม่ต้องจัดทำข้อมูลดังกล่าวขึ้นใหม่ทั้งหมด

/ตารางที่ ๔ ....

ตารางที่ ๔ แนวปฏิบัติในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

กิจกรรม	ผู้มีส่วนได้เสีย		
	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดการเชื่อมโยงและแลกเปลี่ยนข้อมูลตามมาตรฐานเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน	x	x	
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา และตรวจสอบชั้นความลับของข้อมูล	x	x	x
จัดทำแนวทางการทำงานร่วมกันทั้ง ระหว่างหน่วยงานภายในและหน่วยงาน ภายนอกในการเชื่อมโยงและแลกเปลี่ยน ข้อมูล	x	x	
จัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล			x

หมวด ๕ การเปิดเผยข้อมูล

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนาในรูปแบบต่าง ๆ ได้

ผู้มีส่วนได้เสีย

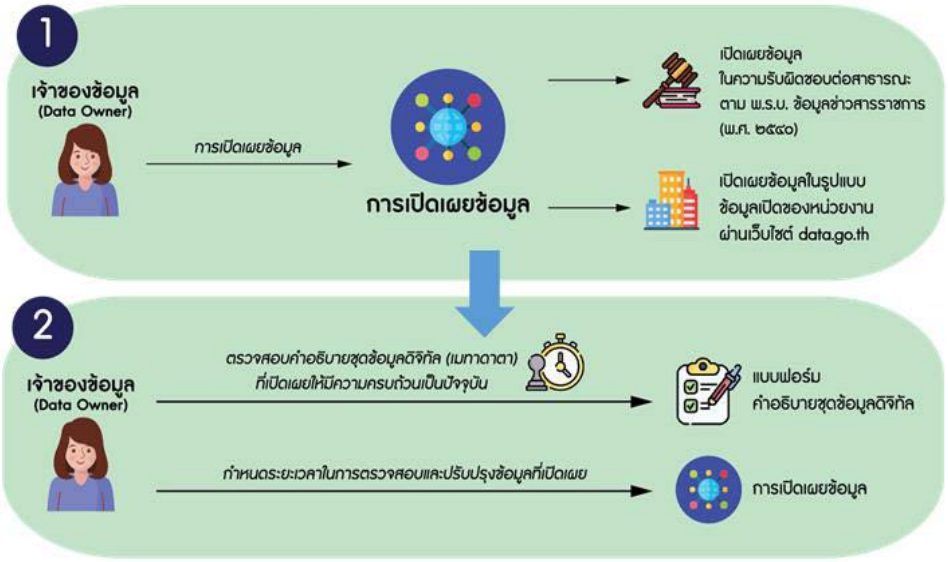
๑) เจ้าของข้อมูล (Data Owners)
๒) ผู้ใช้ข้อมูล (Data Users)
๓) บริกรข้อมูล (Data Stewards)
๔) ผู้ดูแลระบบสารสนเทศ (Systems Administrators)

อ้างอิง

๑. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๒. พระราชบัญญัติข้อมูลข่าวสารราชการ พ.ศ. ๒๕๔๐
๓. พระราชบัญญัติการอำนวยความสะดวกในการพิจารณาอนุญาตของทางราชการ พ.ศ. ๒๕๕๘
๔. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๕. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ

/แนวปฏิบัติ...

แนวปฏิบัติ



๑. เจ้าของข้อมูลจะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ และแนวปฏิบัติการเปิดเผยข้อมูลอย่างเคร่งครัด

๒. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคง และข้อมูลความลับทางราชการที่อยู่ในความครอบครองของสำนักงาน

๓. กำหนดให้เจ้าของข้อมูลที่จะทำการเปิดเผยข้อมูลในความรับผิดชอบในรูปแบบข้อมูลเปิดของสำนักงาน โดยดำเนินการ ดังนี้

(๑) กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้

(๒) กำหนดให้มีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาสำหรับข้อมูลที่ต้องเปิดเผย

(๓) ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน

(๔) ข้อมูลที่เผยแพร่ต้องมาจากแหล่งที่เก็บข้อมูลโดยตรง ด้วยระดับความละเอียดสูง โดยไม่มี การปรับแต่งหรือเป็นข้อมูลรูปแบบสรุป (Summary data)

(๕) ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่ จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐานและกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย

๔. กำหนดให้เงื่อนไขและข้อกำหนดของข้อมูลที่นำมาเปิดเผยภายในเครือข่ายของสำนักงาน ข้อมูลที่ เผยแพร่ต้องไม่ขัดต่อกฎหมายว่าด้วย ทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่ กฎหมายรับรอง

๕. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และต้องเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (Government Open Data) ผ่านเว็บไซต์ data.go.th โดย

(๑) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลที่กำหนดลำดับ

(๒) ชั้นข้อมูลตั้งแต่ลับขึ้นไป อย่างเพียงพอและมีประสิทธิภาพ

(๓) มีการตรวจสอบข้อมูลทีเผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจ ว่าหน่วยงานได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า

/(๔) การเผยแพร่...

(๔) การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด

(๕) หากการเปิดเผยนั้นเป็นการเปิดเผยบนช่องทางที่ดูแลรับผิดชอบโดยหน่วยงานอื่นที่ให้ปฏิบัติตามเอกสาร คู่มือ การนำข้อมูลขึ้นเผยแพร่ของหน่วยงานนั้น

(๖) หากการเปิดเผยข้อมูลไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล และบริกรข้อมูล ทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

๖. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลที่แต่งตั้งโดยหน่วยงานเท่านั้นเว้นแต่คำสั่งนั้นขัดต่อกฎหมาย หรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตาม พ.ร.บ.

๗. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคง และข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงาน รวมทั้ง ห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงาน

๘. กำหนดให้เจ้าของข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูล

๙. กำหนดให้เจ้าของข้อมูลต้องกำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

ตารางที่ ๕ แนวปฏิบัติการเปิดเผยข้อมูล

กิจกรรม	ผู้มีส่วนได้เสีย	
	เจ้าของข้อมูล	บริกรข้อมูล
เปิดเผยข้อมูลสำนักงาน ในความรับผิดชอบต่อสาธารณะตามกฎหมายที่กำหนดไว้ และลงบันทึกเวลา	X	X
คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของข้อมูล	X	
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาของชุดข้อมูลที่จะทำการเปิดเผยให้มีความครบถ้วนเป็นปัจจุบัน	X	X
กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย	X	

หมวด ๖ การทำลายข้อมูล (Data Destroy)

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติการทำลายข้อมูล และการพิจารณาอนุมัติทำลายโดยเจ้าของข้อมูล เพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

ผู้เกี่ยวข้อง/ผู้มีส่วนได้เสีย

๑) เจ้าของข้อมูล (Data Owners)

๒) ผู้ใช้ข้อมูล (Data Users)

๓) ผู้ทำลายข้อมูล (Data Disposers)

๔) ผู้ดูแลระบบสารสนเทศ (Systems Administrators)

๕) บริกรข้อมูล (Data Stewards)

/(๖) เจ้าของข้อมูล...

๖) เจ้าของข้อมูลส่วนบุคคล (Data Subjects)

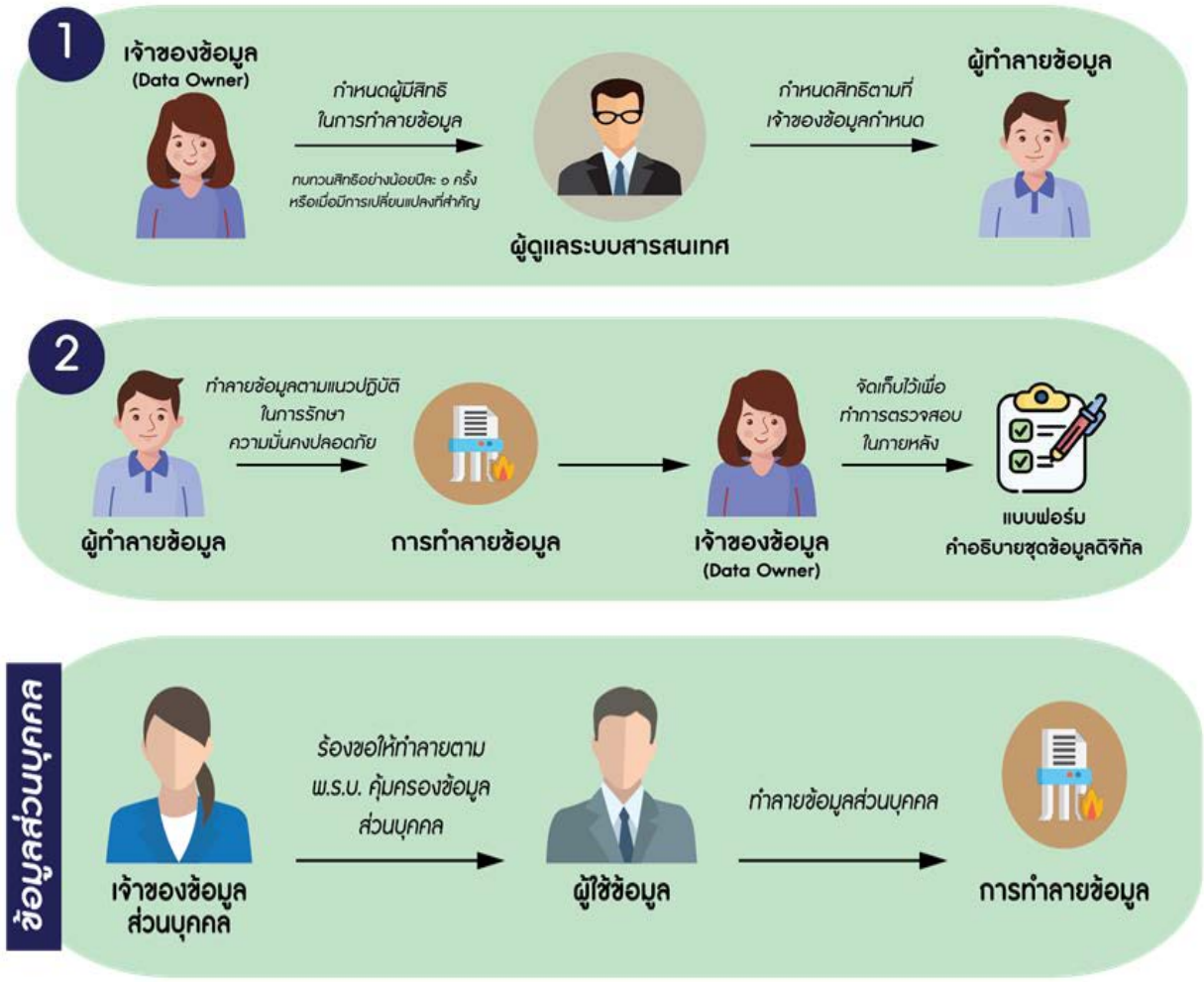
อ้างอิง

๑. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓. ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ISO/IEC ๒๗๐๐๑: ๒๐๑๓

แนวปฏิบัติ



ภาพที่ ๑๐ แนวปฏิบัติการทำลายข้อมูล

๑. เจ้าของข้อมูล (Data Owners) กำหนดระยะเวลาในการจัดเก็บข้อมูลแต่ละประเภท

๒. เจ้าของข้อมูล (Data Owners) กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล และจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

๓. ผู้ดูแลระบบสารสนเทศ (Systems Administrators) กำหนดสิทธิ์ในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูลตามที่ เจ้าของข้อมูลกำหนด และเก็บ Log Files ไว้ด้วยทุกครั้ง

๔. เจ้าของข้อมูล (Data Owners) ต้องจัดเก็บคำอธิบายชุดข้อมูลดิจิทัล (Metadata) ที่ทำลายสำหรับตรวจสอบในภายหลัง

/๕. ผู้ทำลายข้อมูล...

๕. ผู้ทำลายข้อมูล (Data Disposers) ที่ได้รับมอบหมายต้องจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและ บันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี

๖. ผู้ใช้ข้อมูล (Data Users) หรือผู้ประมวลผลข้อมูลส่วนบุคคล ที่ได้รับมอบหมาย สามารถทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคล ร้องขอ (ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล)

๗. บริกรข้อมูล (Data Stewards) ต้องติดตามการดำเนินการเพื่อให้การลบหรือทำลายเป็นไปตามกระบวนการทำลายข้อมูลของหน่วยงาน พร้อมทั้งสรุปรายงานผลประจำเดือน

ตารางที่ ๖ แนวปฏิบัติในการทำลายข้อมูล

กิจกรรม	ผู้มีส่วนได้เสีย				
	เจ้าของข้อมูล	เจ้าของข้อมูลส่วนบุคคล	ผู้ดูแลระบบสารสนเทศ	ผู้ทำลายข้อมูล	บริกรข้อมูล
กำหนดระยะเวลาในการจัดเก็บข้อมูล	X				X
กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล	X				
กำหนดสิทธิ์ในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูลตามที่ เจ้าของข้อมูลกำหนด และเก็บ Log Files ไว้ด้วยทุกครั้ง			X	X	X
จัดเก็บคำอธิบายชุดข้อมูลดิจิทัล (Metadata) ที่ทำลาย สำหรับตรวจสอบในภายหลัง	X		X		X
จัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี			X	X	
ทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคล ร้องขอ (ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล)	X	X	X	X	
ติดตามการดำเนินการลบหรือทำลายเป็นไปตามกระบวนการทำลายข้อมูลของหน่วยงาน พร้อมทั้งสรุปรายงานผลประจำเดือน					X