



คู่มือหลักเกณฑ์และแนวปฏิบัติ สำหรับการบริหารจัดการข้อมูล (ธรรมาภิบาลข้อมูลภาครัฐ)

ศูนย์บริหารข้อมูลอัตลักษณ์บุคคล กองสารสนเทศนิติวิทยาศาสตร์

สถาบันนิติวิทยาศาสตร์ กระทรวงยุติธรรม

ประกาศใช้วันที่ 13 ม.ค. 2568

ประวัติเอกสาร

[illegible]

สารบัญ

1. หลักการและขอบเขต.....	1
2. ผู้มีส่วนได้เสียในการบริหารจัดการข้อมูล.....	2
3. โครงสร้างบุคลากรธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์.....	4
4. บทบาทและหน้าที่ความรับผิดชอบ (Roles and Responsibilities).....	5
5. วงจรชีวิตข้อมูล.....	6
6. หมวดหมู่และการจัดระดับชั้นของข้อมูล.....	7
7. ประเภทข้อมูลที่จัดเก็บ.....	8
8. แนวปฏิบัติในการจัดเก็บข้อมูลไฟล์เอกสาร.....	9
9. แนวปฏิบัติในการเข้าถึงเอกสาร/ข้อมูลและทำสำเนาตามชั้นความลับ.....	10
10. รายชื่อชุดข้อมูลและเจ้าของข้อมูล.....	11
11. แนวปฏิบัติการบริหารจัดการข้อมูล.....	13
หมวด 1 การสร้างข้อมูล.....	13
หมวด 2 การจัดเก็บข้อมูล.....	15
หมวด 3 การประมวลผลข้อมูลและการใช้ข้อมูล.....	18
หมวด 4 การเปิดเผยข้อมูล.....	19
หมวด 5 การทำลายข้อมูล.....	21
หมวด 6 การเชื่อมโยงและการแลกเปลี่ยนข้อมูล.....	22



แนวปฏิบัติการบริหารจัดการข้อมูลสำหรับข้อมูล (ธรรมาภิบาลข้อมูลภาครัฐ)

สถาบันสถิติวิทยา ศาสตร์ กระทรวงยุติธรรม

อ้างอิงพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.2562 กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารงานภาครัฐและการจัดบริการสาธารณะเป็นไปด้วย ความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน รวมทั้งกำหนดให้หน่วยงานของรัฐรวมถึง สถาบันสถิติวิทยา ศาสตร์ ให้มีการบริหารจัดการและ การบูรณาการข้อมูลให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล

การกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในพื้นฐานของธรรมาภิบาลข้อมูลภาครัฐ ดังนั้นเพื่อให้ธรรมาภิบาลข้อมูลภาครัฐมีประสิทธิภาพ สถาบันสถิติวิทยา ศาสตร์จึงจัดทำนโยบายข้อมูลและประกาศบังคับใช้ให้ข้าราชการ พนักงานราชการ และเจ้าหน้าที่ผู้ปฏิบัติงานทราบโดยทั่วกัน แต่อย่างไรก็ดีเพื่อให้ข้าราชการ พนักงานราชการ และเจ้าหน้าที่ผู้ปฏิบัติงานสามารถดำเนินงานอย่างมีประสิทธิภาพมากขึ้นและเป็นไปตามนโยบายที่กำหนด สถาบันสถิติวิทยา ศาสตร์จึงจัดทำแนวปฏิบัติฉบับนี้เพื่อเป็นแนวทางในการบริหารจัดการข้อมูล จัดหา นำเข้าข้อมูล เข้าถึง ใช้ประมวลผลข้อมูล ทำลายข้อมูล เผยแพร่ข้อมูล รวมไปถึงเพิ่มเติมข้อควรปฏิบัติและไม่ควรปฏิบัติ และเกณฑ์ต่างๆ

1. หลักการและขอบเขต

แนวปฏิบัติการบริหารจัดการข้อมูลนี้ จัดทำขึ้นเพื่อให้ผู้ปฏิบัติงาน ดำเนินงานได้สอดคล้องตามนโยบายธรรมาภิบาลข้อมูลภาครัฐ (Data Policy) ที่ สถาบันสถิติวิทยา ศาสตร์ประกาศ ซึ่งเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูลภาครัฐ นำมาซึ่งการเก็บ ใช้ เผยแพร่ และทำลายข้อมูล โดยที่ไม่กระทบสิทธิของเจ้าของข้อมูลหรือก่อให้เกิดความเสียหายและใช้มาตรฐานเดียวกันทั้งองค์กร มีผลบังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามแนวปฏิบัติที่สถาบันสถิติวิทยา ศาสตร์ประกาศ ซึ่งมีหน้าที่โดยตรงที่จะต้องสนับสนุน ดำเนินการและปฏิบัติตามอย่างเคร่งครัด โดยแนวปฏิบัติจะครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูลและองค์ประกอบในการบริหารจัดการข้อมูล ดังต่อไปนี้



2. ผู้มีส่วนได้เสียในการบริหารจัดการข้อมูล

ทั้งนี้แนวปฏิบัติเกี่ยวกับข้อมูลนี้บังคับใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับข้อมูลตามประกาศแนวปฏิบัติการบริหารจัดการข้อมูลของสถาบันนิติวิทยาศาสตร์ รวมถึงผู้เกี่ยวข้องอื่น ๆ ที่ไม่ได้ระบุไว้ใน แนวปฏิบัติ ดังคำนิยาม



ภาพที่ 1 ผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูล
(ที่มา ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องธรรมาภิบาลข้อมูลภาครัฐ)

คำนิยาม

การประมวลผลข้อมูล	การดำเนินการใดๆ ซึ่งกระทำต่อข้อมูลหรือชุดข้อมูลไม่ว่าจะโดยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บบันทึก จัดระบบ จัดโครงสร้างเก็บรักษา เปลี่ยนแปลงหรือปรับเปลี่ยน การรับพิจารณาใช้เปิดเผยด้วยการส่งต่อ เผยแพร่ หรือการกระทำอื่นใดซึ่งทำให้เกิดความพร้อมใช้งาน การจัดวางหรือ ผสมเข้าด้วยกัน การจำกัด การลบ หรือการทำลาย
การลบข้อมูลแบบถาวร	การลบข้อมูลอิเล็กทรอนิกส์ที่ไม่สามารถกู้ข้อมูลที่ลบแล้วกลับคืนมาได้โดย การเลือกใช้เครื่องมือที่เหมาะสมในการลบข้อมูล
ข้อมูล (Data)	ข้อมูลทุกประเภทที่มีการบันทึก และ/หรือ ประมวลผลและถูกจัดเก็บไว้ใน ฐานข้อมูลในระบบงานต่างๆ ของสถาบันนิติวิทยาศาสตร์
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือ ทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (พ.ร.บ.คุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562)
ชุดข้อมูล (Dataset)	การนำข้อมูลจากหลายแหล่งมารวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะ โครงสร้างของข้อมูล

คลังเอกสาร	สถานที่จัดเก็บเอกสารสำคัญของสถาบันนิติวิทยาศาสตร์
ผู้สร้างข้อมูล (Data Creators)	พนักงานและผู้ปฏิบัติงานที่มีหน้าที่ บันทึก แก้ไข ปรับปรุงหรือลบข้อมูลให้สอดคล้องกับมาตรฐานที่สถาบันกำหนด
ผู้ใช้ข้อมูล (Data User)	พนักงานและผู้ปฏิบัติงานที่มีหน้าที่และความรับผิดชอบหรือมีสิทธิในการใช้ข้อมูลในการปฏิบัติงานประจำวันตามที่ได้รับอนุญาตภายใต้ขอบเขตที่กำหนด
เจ้าของข้อมูล (Data Owner)	ผู้ที่ได้รับมอบหมายในปฏิบัติงานให้รับผิดชอบข้อมูลที่ระบุไว้ ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยทำหน้าที่กำกับดูแลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูลนั้นๆ รวมทั้งทำหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล
ทีมบริหารจัดการข้อมูล (Data Management Team)	กลุ่มบุคคลในกองสารสนเทศนิติวิทยาศาสตร์ที่ทำหน้าที่รับผิดชอบดูแลรักษาข้อมูลในระบบสารสนเทศของหน่วยงาน และสนับสนุนกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐ เช่น ช่วยเหลือในการนิยามเมทาดาตา ร่างนโยบายข้อมูล และมาตรฐานข้อมูล และกำหนดสิทธิการเข้าถึงข้อมูลในระบบ
ผู้ดูแลระบบสารสนเทศ (System Administrators)	บุคลากรที่มีหน้าที่ดูแลรับผิดชอบระบบสารสนเทศของหน่วยงาน
ผู้ดูแลระบบแม่ข่าย (Server Administrators)	บุคลากรที่มีหน้าที่ดูแลรับผิดชอบระบบแม่ข่ายของหน่วยงาน
ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ทำลายข้อมูล (Data Destroyers)	บุคลากรที่ได้รับการกำหนดสิทธิจากเจ้าของข้อมูลให้มีสิทธิในการทำลายข้อมูล
เจ้าของระบบงาน (Application Owner)	ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในหน่วยงาน รวมถึงผู้บังคับบัญชาของเจ้าของระบบงานนั้นด้วย
เจ้าของข้อมูลส่วนบุคคล (Data Subject)	บุคคลธรรมดาที่ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลนั้นระบุถึง
คณะกรรมการ ธรรมาภิบาลข้อมูล (Data Governance Concil)	คณะกรรมการกำกับดูแลข้อมูลตามคำสั่งแต่งตั้งของสถาบันนิติวิทยาศาสตร์
คณะทำงานทีมบริการข้อมูล (Data Steward Team)	ผู้ที่ได้รับมอบหมาย ซึ่งอาจเป็นตัวแทนของเจ้าของข้อมูลในการจัดการข้อมูล เพื่อให้ข้อมูลมีคุณภาพตามมาตรฐานของสถาบันนิติวิทยาศาสตร์



3. โครงสร้างบุคลากรธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์

3.1 โครงสร้างคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ประกอบด้วย

- 1) ประธานกรรมการ ได้แก่ ผู้อำนวยการสถาบันนิติวิทยาศาสตร์
- 2) รองประธานกรรมการ ได้แก่ รองผู้อำนวยการสถาบันนิติวิทยาศาสตร์ ที่รับผิดชอบตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)
- 3) กรรมการโดยตำแหน่ง อย่างน้อยจำนวน 13 คน ได้แก่ ผู้เชี่ยวชาญ ผู้อำนวยการหรือหัวหน้ากลุ่มจากหน่วยงานต่อไปนี้
 - รองผู้อำนวยการสถาบันนิติวิทยาศาสตร์
 - ผู้เชี่ยวชาญเฉพาะด้านนิติวิทยาศาสตร์
 - ผู้เชี่ยวชาญเฉพาะด้านนิติเวช
 - กองนิติวิทยาศาสตร์บริการ
 - กองตรวจพิสูจน์ทางวิทยาศาสตร์
 - กองปฏิบัติการพิเศษทางนิติวิทยาศาสตร์
 - กองมาตรฐานนิติวิทยาศาสตร์
 - กองพัฒนาระบบติดตามคนหายและการพิสูจน์ศพนิรนาม
 - กองกิจการต่างประเทศและส่งเสริมงานด้านนิติวิทยาศาสตร์
 - กองสารพันธุกรรม
 - เลขาธิการกรม
 - กลุ่มพัฒนาระบบบริหาร
 - กองสารสนเทศนิติวิทยาศาสตร์
- 4) ให้ผู้อำนวยการกองสารสนเทศนิติวิทยาศาสตร์เป็นเลขานุการ และให้แต่งตั้งเจ้าหน้าที่เป็นผู้ช่วยเลขานุการได้ไม่เกิน 3 คน

3.2 โครงสร้างคณะทำงานทีมบริการข้อมูล (Data Steward Team) ประกอบด้วย

- 1) ประธานคณะทำงานทีมบริการข้อมูล ได้แก่ ผู้อำนวยการกองสารสนเทศนิติวิทยาศาสตร์
- 2) รองประธานคณะทำงาน ได้แก่ ผู้ที่มีอาวุโสมากที่สุดจากรายชื่อที่แต่ละกองเสนอมา
- 3) คณะทำงาน ได้แก่ ผู้แทนจากทุกหน่วยงานตามโครงสร้างองค์กรกองละ 1 คนเป็นอย่างน้อย
- 4) ให้ผู้แทนจากกองสารสนเทศนิติวิทยาศาสตร์เป็นเลขานุการ และให้แต่งตั้งเจ้าหน้าที่ของสถาบันเป็นผู้ช่วยเลขานุการได้ไม่เกิน 3 คน



4. บทบาทและหน้าที่ความรับผิดชอบ (Roles and Responsibilities)

4.1 คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) มีอำนาจหน้าที่ดังนี้

- (1) กำหนดนโยบายธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์
- (2) กำหนดระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่นๆ ที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์
- (3) กำกับติดตามการดำเนินงาน แก้ไขปัญหาและบริหารจัดการธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์
- (4) กำหนดแนวทางเกี่ยวกับมาตรฐานการวัดคุณภาพ มาตรฐานความมั่นคงปลอดภัย ระดับชั้นความลับ รวมถึงการจัดลำดับความสำคัญของข้อมูลในการกำกับดูแล
- (5) กำหนดบทบาทหน้าที่และขอบเขตของผู้มีส่วนได้ส่วนเสียของข้อมูลภายในสถาบันนิติวิทยาศาสตร์ในการบริหารจัดการข้อมูล
- (6) ทบทวนนโยบายธรรมาภิบาลข้อมูล รวมถึงระเบียบ ข้อบังคับ คำสั่งหรือข้อกำหนดอื่นๆ อย่างน้อยปีละ 1 ครั้ง และดำเนินการปรับปรุงอย่างต่อเนื่อง
- (7) สนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนัก และความเข้าใจในธรรมาภิบาลข้อมูล ภาครัฐและการบริหารจัดการข้อมูล โดยให้ครอบคลุมทุกกระบวนการของการบริหารจัดการข้อมูล
- (8) สื่อสาร เผยแพร่ สร้างความรู้ความเข้าใจ และประชาสัมพันธ์นโยบายธรรมาภิบาลข้อมูลให้กับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกสถาบันนิติวิทยาศาสตร์ทราบ

4.2 คณะทำงานทีมบริการข้อมูล (Data Steward Team) มีอำนาจหน้าที่ดังนี้

- (1) เสนอแนะเชิงนโยบาย และร่างนโยบายธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์แก่คณะกรรมการธรรมาภิบาลข้อมูลสถาบันนิติวิทยาศาสตร์
- (2) เสนอแนะแนวทางและร่างระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่นๆ ที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์แก่คณะกรรมการธรรมาภิบาลข้อมูลสถาบันนิติวิทยาศาสตร์
- (3) เสนอแนะแนวทางแก้ไขปัญหาและแนวทาง การบริหารจัดการธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์แก่คณะกรรมการธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์
- (4) เสนอแนะแนวทางเกี่ยวกับมาตรฐานการวัดคุณภาพ มาตรฐานความมั่นคงปลอดภัย ระดับชั้นความลับรวมถึงการจัดลำดับความสำคัญของข้อมูลในการกำกับดูแลแก่คณะกรรมการธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์
- (5) เสนอแนะบทบาทหน้าที่และขอบเขตของผู้มีส่วนได้ส่วนเสีย ของข้อมูลภายในสถาบันนิติวิทยาศาสตร์ในการบริหารจัดการข้อมูลแก่คณะกรรมการธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์
- (6) ตรวจสอบความสอดคล้องกันระหว่างนโยบายข้อมูลกับการดำเนินการใดๆ ของผู้มีส่วนได้ส่วนเสีย อย่างน้อยปีละ 1 ครั้ง



(7) เสนอแนะแนวทางการทบทวนนโยบายธรรมาภิบาลข้อมูลแก่คณะกรรมการธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์

(8) ปฏิบัติการอื่นใดที่ได้รับมอบหมายจากคณะกรรมการธรรมาภิบาลข้อมูลของสถาบันนิติวิทยาศาสตร์

5. วงจรชีวิตข้อมูล

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

5.2 การจัดเก็บข้อมูล (Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือข้อมูลที่ได้จากการเชื่อมโยงและ/หรือแลกเปลี่ยนกับหน่วยงานอื่น ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS) เพื่อให้เกิดความมีระเบียบง่ายต่อการใช้งาน ข้อมูลไม่สูญหายหรือถูกทำลาย และช่วยให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว

5.3 การประมวลผลและใช้ข้อมูล (Processing and Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

5.4 การเผยแพร่ข้อมูล (Disclosure) เป็นการนำข้อมูลที่อยู่ในความครอบครองของหน่วยงานเผยแพร่ตามช่องทางต่าง ๆ อย่างเหมาะสม อาทิ การเปิดเผยข้อมูล (Open data) การแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition)

5.5 กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการย้ายข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อเก็บรักษาถาวรโดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

5.6 การทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

5.7 การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Linkage and Exchange) การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานทั้งภายในและภายนอกให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ



ภาพที่ 2 แสดงวงจรชีวิตของข้อมูล

(ที่มา ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องธรรมาภิบาลข้อมูลภาครัฐ)

6. หมวดหมู่และการจัดระดับชั้นของข้อมูล

ข้อมูลของ สถาบันนิติวิทยาศาสตร์ กำหนดแบ่งหมวดหมู่ และระดับชั้นความลับ ใช้งานภายใน ดังนี้

หมวดที่ 1 ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล ที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้นๆ ได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

หมวดที่ 2 ข้อมูลความมั่นคง หมายถึง ข้อมูลเกี่ยวกับความมั่นคงของรัฐที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น

หมวดที่ 3 ข้อมูลความลับทางราชการ หมายถึง ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล

หมวดที่ 4 ข้อมูลสาธารณะ หมายถึง ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ

โดยมีการจัดระดับชั้นความลับของข้อมูล ดังนี้

- ข้อมูลใช้ภายใน (Internal Use Only) ได้แก่ ข้อมูลสำหรับการดำเนินการภายในของหน่วยงานซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต เช่น มาตรฐานและขั้นตอนการปฏิบัติงาน ประกาศและบันทึกภายในหน่วยงาน เป็นต้น
- ข้อมูลที่มีชั้นความลับ (Secret) แบ่งเป็น ข้อมูลลับที่สุด (Top Secret) ข้อมูลลับมาก (Secret) และ ข้อมูลลับ (Confidential)
- ข้อมูลเปิดเผยได้ (Public) ได้แก่ ข้อมูลที่สามารถเปิดเผยได้แก่บุคคลทั่วไป เช่น ข้อมูลเผยแพร่บนเว็บไซต์ ข้อมูลจากการแถลงข่าว สถิติหรือรายงานประจำปีของหน่วยงาน เป็นต้น



ภาพที่ 3 แสดงระดับชั้นความลับของข้อมูล

(ที่มา ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องธรรมาภิบาลข้อมูลภาครัฐ)

7. ประเภทข้อมูลที่จัดเก็บ สามารถแบ่งประเภทข้อมูลเป็น 2 ประเภท ดังนี้

7.1 ข้อมูลเอกสารกระดาษ แบ่งได้ 3 กลุ่ม ได้แก่

(1) เอกสารที่มีข้อกำหนดทางการ หรือมีผลทางกฎหมาย เป็นเอกสารที่มีคำสั่งจากหน่วยงานราชการหรือกฎหมาย มีข้อกำหนดวิธีการจัดเก็บเอกสารชัดเจนหรือเป็นเอกสารที่ใช้ในการฟ้องร้องดำเนินคดี หรือเป็นเอกสารการสมัครใช้บริการ

(2) เอกสารผู้ขอรับบริการหรือเอกสารที่มีการขอใช้บ่อยครั้ง เป็นเอกสารของผู้ขอรับบริการหรือเอกสารที่ผู้ขอรับบริการขอใช้งานบ่อยครั้ง เช่น ใบเสร็จรับเงิน, ใบคำขอเปลี่ยนแปลงข้อมูล เป็นต้น

(3) เอกสารภายใน สถาบันนิติวิทยาศาสตร์ เป็นเอกสารแจ้งดำเนินการระหว่างหน่วยงานหรือเอกสารดำเนินการของหน่วยงานภายในสถาบันนิติวิทยาศาสตร์ เช่น รายงานประจำวัน, ทะเบียนคุมต่างๆ เป็นต้น

7.2 ข้อมูลอิเล็กทรอนิกส์ แบ่งได้ 6 กลุ่ม

(1) ได้แก่เอกสารภาพจากการสแกน (Image) หรือไฟล์ภาพ เช่น ภาพสแกนเอกสารผู้ขอรับบริการ เช่น สำเนาบัตรประชาชน, ภาพสแกนใบคำขอสมัครใช้บริการ เป็นต้น

(2) ข้อมูลที่ผ่านช่องทางอิเล็กทรอนิกส์ (Digital) เป็นข้อมูลจากผู้ขอรับบริการทำการเองเข้ามาจากช่องทาง Digital หรือข้อมูลที่เจ้าหน้าที่ทำการการเพิ่มเติมในระบบงานต่าง ๆ ของสถาบันนิติวิทยาศาสตร์ เช่น ข้อมูลการสมัคร eService, ข้อมูลการทำรายการผ่านเว็บไซต์ของสถาบันนิติวิทยาศาสตร์ เป็นต้น

(3) Security Log เป็นข้อมูลที่มีการเก็บบันทึกไว้เพื่อใช้ในการดำเนินการกำกับดูแลความมั่นคงปลอดภัยของระบบ (Security Governance)

(4) ข้อมูลภาพหรือเสียงเกี่ยวกับการรักษาความปลอดภัย (Security) หรือการติดต่อจากผู้ขอรับบริการ เป็นภาพที่ได้จากการบันทึก ข้อมูลในกล้องวงจรปิดหรือเสียงจากการติดต่อจากผู้ขอรับบริการ เช่น IVR, Call Center เป็นต้น

(5) ข้อมูลในฐานะข้อมูลสถาบันนิติวิทยาศาสตร์ เป็นถึงข้อมูลของสถาบันนิติวิทยาศาสตร์ เช่น ฐานข้อมูล eService ฐานข้อมูลคนหาย คนนิรนามและศพนิรนาม ฐานข้อมูลสารพันธุกรรม เป็นต้น

(6) ข้อมูลในคอมพิวเตอร์ส่วนบุคคล เป็นข้อมูลที่ติงมาจากระบบต่าง ๆ มาทำงานที่เครื่องส่วนบุคคล ข้อมูลหรือรายงานที่แต่ละหน่วยงานมีการจัดทำขึ้นเพื่อใช้ในงาน เป็นต้น

8. แนวปฏิบัติในการจัดเก็บข้อมูลไฟล์เอกสาร

8.1 ช่องทางการจัดเก็บเอกสาร โดยจำแนกตามประเภทของเอกสาร ดังนี้

(1) เอกสารราชการ

ให้สแกนเก็บไฟล์เอกสารเข้าระบบสารบรรณอิเล็กทรอนิกส์ E-saraban ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) โดยพื้นที่จัดเก็บอยู่ที่ Cloud ภาครัฐ

(2) เอกสารคุณภาพ

2.1 เอกสารที่ดำเนินการเกี่ยวกับคุณภาพต่างๆ ระเบียบปฏิบัติ แนวทางปฏิบัติและอื่นๆ ที่เกี่ยวข้อง จัดเก็บในระบบ E-Document Control

2.2 ให้การดำเนินการตามแนวทางของกองมาตรฐานนิติวิทยาศาสตร์

(3) เอกสารรายงานผลการตรวจพิสูจน์/เอกสารทางคดี

3.1 เก็บไว้ฐานข้อมูลรายงานในระบบเชื่อมโยง

3.2 ให้หน่วยงานเก็บไฟล์รายงานฯ ย้อนหลังนำเข้าผ่านระบบเชื่อมโยงได้ที่ fis.cifs.go.th

8.2 หน้าที่ความรับผิดชอบ

(1) หน่วยงานตรวจพิสูจน์ (หน่วยงานเจ้าของเอกสารรายงาน)

1.1 ให้ดำเนินการสแกน และเป็นผู้นำไฟล์ เข้าฐานข้อมูล โดยต้องตรวจสอบความถูกต้องครบถ้วน สมบูรณ์

1.2 กรณีที่มีการประสานให้บริษัทช่วยดำเนินการในทางเทคนิค เป็นความรับผิดชอบ
หน่วยงานต้องดำเนินการ ตรวจสอบความถูกต้อง ครบถ้วน สมบูรณ์

(2) ศูนย์ข้อมูลกลางฯ

2.1 ดูแลรักษาความมั่นคงปลอดภัยข้อมูล

2.2 ทำสำเนาตามที่อยู่อาศัยการสถาบันนิติวิทยาศาสตร์พิจารณา

2.3 และถ้าค้นหาไฟล์ ไม่พบในฐานข้อมูล ให้ดำเนินการแจ้งหน่วยงานตรวจพิสูจน์ดำเนินการ
ตรวจสอบและสแกนนำเข้า

9. แนวปฏิบัติในการเข้าถึงเอกสาร/ข้อมูลและทำสำเนาตามชั้นความลับ

ระดับ	การเข้าถึงเอกสาร/ข้อมูล	การทำสำเนาเอกสาร/ส่งต่อข้อมูล
ใช้ภายใน	เอกสาร/ข้อมูลต้องสามารถเข้าถึงได้โดย เจ้าหน้าที่สถาบันนิติวิทยาศาสตร์เท่านั้น	ไม่อนุญาตให้ทำสำเนาและส่งต่อให้ผู้อื่นที่ไม่ เกี่ยวข้อง ยกเว้นได้รับอนุญาตอย่างมีลาย ลักษณ์อักษร
ลับที่สุด	เอกสาร/ข้อมูลต้องสามารถเข้าถึงได้โดย บุคคลที่ได้รับสิทธิ์เท่านั้น โดยสิทธิ์ดังกล่าว ต้องถูกกำหนดไว้อย่างชัดเจนโดย คณะกรรมการและต้องสามารถตรวจสอบได้	ไม่อนุญาตให้ทำสำเนาและส่งต่อให้ผู้อื่นที่ไม่ เกี่ยวข้อง ยกเว้นได้รับอนุญาตอย่างมีลาย ลักษณ์อักษร และจัดให้มีการทำทะเบียน บันทึกผู้ทำสำเนา/Log
ลับมาก	เอกสาร/ข้อมูลต้องสามารถเข้าถึงได้โดย บุคคลที่ได้รับสิทธิ์เท่านั้น โดยสิทธิ์ดังกล่าว ต้องถูกกำหนดไว้อย่างชัดเจนโดย คณะกรรมการและต้องสามารถตรวจสอบได้	ไม่อนุญาตให้ทำสำเนาและส่งต่อให้ผู้อื่นที่ไม่ เกี่ยวข้อง ยกเว้นได้รับอนุญาตอย่างมีลาย ลักษณ์อักษร
ลับ	เอกสาร/ข้อมูลต้องสามารถเข้าถึงได้โดย บุคคลที่ได้รับสิทธิ์เท่านั้น โดยสิทธิ์ดังกล่าว ต้องถูกกำหนดไว้อย่างชัดเจนโดยเจ้าของ ข้อมูลและต้องสามารถตรวจสอบได้	อนุญาตให้ทำสำเนาและส่งต่อให้ผู้อื่นได้ เพื่อ ใช้ในการปฏิบัติงานเท่านั้น
สาธารณะ/ เปิดเผย	ไม่มีข้อจำกัด	ไม่มีข้อจำกัด



10. รายชื่อชุดข้อมูลและเจ้าของข้อมูล

คณะกรรมการธรรมาภิบาลข้อมูลภาครัฐของสถาบันนิติวิทยาศาสตร์ ได้กำหนดรายชื่อชุดข้อมูลสำคัญของสถาบันนิติวิทยาศาสตร์และหน่วยงานเจ้าของชุดข้อมูล ให้ดำเนินการจัดทำข้อมูลเปิดภาครัฐเพื่อใช้ในการปฏิบัติงานในองค์กร การวิเคราะห์ การกำหนดนโยบาย การออกแบบบริการ หรือใช้ประกอบการตัดสินใจ และนำข้อมูลมาใช้ประโยชน์ จำนวน 5 ด้าน ดังนี้

ชุดข้อมูล	หน่วยงานเจ้าของชุดข้อมูล
1. ด้านการสนับสนุน	
• ข้อมูลยุทธศาสตร์และแผนงาน	กลุ่มนโยบายและแผน
• ข้อมูลกฎหมาย ระเบียบ ข้อบังคับ	กลุ่มกฎหมายและนิติการ
• ข้อมูลโครงสร้างองค์กร อัตรากำลัง	กลุ่มงานการเจ้าหน้าที่/กลุ่มพัฒนาระบบบริหาร
• ข้อมูลบุคลากร	กลุ่มงานการเจ้าหน้าที่
• ข้อมูลการพัฒนาบุคลากร	กลุ่มพัฒนาบุคลากร
• ข้อมูลงบประมาณ การเงิน	กลุ่มงานการคลัง
• ข้อมูลการจัดซื้อ จัดจ้าง	กลุ่มงานพัสดุ
• ข้อมูลวัสดุและครุภัณฑ์	กลุ่มงานพัสดุ
• ข้อมูลสัญญา	กลุ่มงานพัสดุ
• ข้อมูลประชาสัมพันธ์	กลุ่มประชาสัมพันธ์และสื่อสารองค์กร
• ข้อมูลคำสั่งต่างๆ	สำนักงานเลขานุการกรม
2. ด้านคุณภาพมาตรฐาน	
• ข้อมูลมาตรฐานสากลและกระบวนการ	กองมาตรฐานนิติวิทยาศาสตร์
• ข้อมูลความไม่สอดคล้องในการดำเนินงานตามมาตรฐาน	กองมาตรฐานนิติวิทยาศาสตร์
• ข้อมูลการได้รับรางวัล	กลุ่มพัฒนาระบบบริหาร
• ข้อมูลความร่วมมือ MOU	กองกิจการต่างประเทศและส่งเสริมงานด้านนิติวิทยาศาสตร์
• ข้อมูลการร้องเรียน	กลุ่มงานจริยธรรม/ศูนย์บริการร่วม OneStopService
• ข้อมูลการควบคุมภายใน	กลุ่มตรวจสอบภายใน
• ข้อมูลความเสี่ยง	กองมาตรฐานนิติวิทยาศาสตร์
• ข้อมูลด้านอาชีวอนามัยและความปลอดภัย	กองมาตรฐานนิติวิทยาศาสตร์

ชุดข้อมูล	หน่วยงานเจ้าของชุดข้อมูล
3. ด้านวิชาการ	
• ข้อมูลองค์ความรู้	ทุกหน่วยงาน
• ข้อมูลงานวิจัย	กลุ่มบริหารงานวิจัย
• ข้อมูลบริการเผยแพร่เพื่อการทำวิจัย	กลุ่มบริหารงานวิจัย
4. ด้านการให้บริการและการตรวจพิสูจน์	
• ข้อมูลรับแจ้งเหตุ	หน่วยรับแจ้ง กลุ่มนิติพยาธิ
• ข้อมูลวัตถุพยาน	กลุ่มบริหารจัดการวัตถุพยาน
• ข้อมูลขอบริการตรวจพิสูจน์ภาคประชาชน 3 ด้าน	ศูนย์บริการร่วม OneStopService
• ข้อมูลการร้องทุกข์	ศูนย์บริการร่วม OneStopService
• ข้อมูลบริการตรวจสถานที่เกิดเหตุ ส่วนกลาง	กลุ่มปฏิบัติการทางนิติวิทยาศาสตร์ ส่วนกลาง
• ข้อมูลบริการตรวจสถานที่เกิดเหตุ ส่วนภูมิภาค	กลุ่มปฏิบัติการทางนิติวิทยาศาสตร์ ส่วนภูมิภาค
• ข้อมูลบริการติดตามคนหาย และการพิสูจน์คนนิรนามและศพนิรนาม	กองพัฒนาระบบติดตามคนหายและการพิสูจน์ศพนิรนาม
• ข้อมูลบริการนิติจิตเวช	กลุ่มนิติจิตเวช
• ข้อมูลบริการนิติเวชคลินิก	กลุ่มนิติเวชคลินิก
• ข้อมูลบริการนิติพยาธิ และตรวจพิสูจน์ชั้นสูตรศพ	กลุ่มนิติพยาธิวิทยา
• ข้อมูลตรวจพิสูจน์อาวุธปืนและฟิสิกส์	กลุ่มตรวจพิสูจน์อาวุธปืนและวัตถุพยานทางฟิสิกส์
• ข้อมูลตรวจพิสูจน์เอกสาร	กลุ่มตรวจพิสูจน์พยานเอกสาร
• ข้อมูลตรวจพิสูจน์เคมี	กลุ่มตรวจพิสูจน์ทางเคมี
• ข้อมูลตรวจพิสูจน์ลายนิ้วมือ	กลุ่มตรวจพิสูจน์ลายนิ้วมือ
• ข้อมูลตรวจพิสูจน์อิเล็กทรอนิกส์	กลุ่มตรวจพิสูจน์พยานหลักฐานทางอิเล็กทรอนิกส์
• ข้อมูลตรวจพิสูจน์สารพันธุกรรม	กองสารพันธุกรรม
• ข้อมูลตรวจพิสูจน์กระดูก	กลุ่มตรวจพิสูจน์กระดูก
• ข้อมูลไฟล์รายงานผลการตรวจพิสูจน์	ทุกหน่วยตรวจพิสูจน์
• ข้อมูลการตรวจพิสูจน์และวิจัยด้านการจราจร	ศูนย์ตรวจพิสูจน์และวิจัยด้านการจราจร
• ข้อมูลสถิติการให้บริการ	ทุกหน่วยงาน



ชุดข้อมูล	หน่วยงานเจ้าของชุดข้อมูล
5. ด้านการวัดและประเมินผล	
• ข้อมูลการประเมินความพึงพอใจ	ภายนอก หน่วยงานที่ให้บริการภายนอก ภายใน กองมาตรฐานนิติวิทยาศาสตร์
• ข้อมูลตัวชี้วัด แบ่งเป็น ระดับ สำนักงาน กพร. กระทรวง กรม กอง	กลุ่มพัฒนาระบบบริหาร

11. แนวปฏิบัติการบริหารจัดการข้อมูล

แนวปฏิบัติการบริหารจัดการข้อมูลตามวงจรชีวิตข้อมูล แบ่งออกเป็น 6 หมวด ได้แก่ การสร้างข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูลและการใช้ข้อมูล การเชื่อมโยงและการแลกเปลี่ยนข้อมูล การเปิดเผยข้อมูล และการทำลายข้อมูล ในแต่ละหมวดจะระบุ วัตถุประสงค์ ผู้รับผิดชอบงาน อ้างอิง และข้อปฏิบัติ และตารางแสดงความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย ซึ่งหน่วยงานสามารถกำหนดข้อปฏิบัติอื่น ๆ เพิ่มเติมให้สอดคล้องกับสภาพแวดล้อมและวัฒนธรรมองค์กร และจะต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง

หมวด 1 การสร้างข้อมูล การจัดเก็บ และการทำลายข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการสร้างข้อมูลให้มีคุณภาพ มีความมั่นคงปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

ผู้รับผิดชอบงาน

1. ผู้สร้างข้อมูล (Data Creators)
2. ทีมบริหารจัดการข้อมูล (Data Management Team)
3. เจ้าของข้อมูล (Data Owners)
4. บริกรข้อมูล (Data Stewards)
5. ผู้ดูแลระบบสารสนเทศ (System Administrators)

ข้อปฏิบัติ

1. เจ้าของข้อมูล (ไม่ว่า เจ้าของข้อมูล จะอยู่ภายใน กอง/สำนัก/ฝ่าย/ศูนย์ เดียว หรือ มากกว่าหลาย กอง /สำนัก/ฝ่าย/ศูนย์ ต้องมีการกำหนดชัดเจน ถึงอำนาจหน้าที่และขั้นตอนการทำงานร่วมกัน)

1.1 กำหนดผู้มีสิทธิในการสร้างข้อมูล และจะต้องทบทวนสิทธินั้น อย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

1.2 กำหนดหมวดหมู่และชั้นความลับของข้อมูล



2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด

3. เจ้าของข้อมูล บริการข้อมูลธุรกิจ บริการข้อมูลเทคนิค และทีมบริหารจัดการข้อมูล ร่วมจัดทำ คำอธิบาย ชุดข้อมูลดิจิทัลหรือเมทาดาทา (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานขั้นต่ำคำอธิบายชุดข้อมูลดิจิทัลที่สำนักงานพัฒนารัฐบาลดิจิทัล (สปร.) กำหนด และกำหนดให้ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมินคุณค่าชุดข้อมูลที่ สปร. หรือหน่วยงานกำหนด เพื่อสนับสนุนการคัดเลือกเป็นชุดข้อมูลคุณค่าสูง (High Value Dataset) และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล

4. ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะดังต่อไปนี้เข้าสู่ระบบคอมพิวเตอร์ที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

- ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน
- ข้อมูลอันเป็นเท็จ ที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือ โครงสร้างพื้นฐาน หรือ ก่อให้เกิดความตื่นตระหนก
- ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือ ความผิดเกี่ยวกับการก่อการร้าย
- ข้อมูลที่มีลักษณะอันลามก และอาจเข้าถึงได้
- ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือ ได้รับความอับอาย

5. ห้ามมิให้ผู้สร้างข้อมูล ทำการสร้าง/ทำซ้ำต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น เว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง

6. กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น

7. กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น

หมวด 2 การจัดเก็บข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติสำหรับผู้ที่เกี่ยวข้องในการจัดเก็บข้อมูล ให้มีคุณภาพ เข้าถึงและใช้งานได้อย่างมั่นคงปลอดภัย

ผู้รับผิดชอบงาน

1. เจ้าของข้อมูล (Data Owners)
2. ผู้ดูแลระบบสารสนเทศ (System Administrators)
3. ผู้สร้างข้อมูล (Data Creators)
4. บริกรข้อมูล (Data Stewards)
5. ผู้ใช้ข้อมูล (Data Users)
6. ทีมบริหารจัดการข้อมูล (Data Management Team)

ข้อปฏิบัติ

1. กำหนดให้เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน
2. กำหนดให้ทีมบริหารจัดการข้อมูล และผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้วเพื่อจัดเก็บเป็นข้อมูลถาวร
3. กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาเดตา หากไม่มีหรือ ไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูล บริกรข้อมูล โดยทีมบริหารจัดการข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน
4. ผู้มีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูล ทั้งเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และทีมบริหารจัดการข้อมูล จะต้องจัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน โดยทำการเข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้การเข้ารหัสข้อมูลให้ปฏิบัติตามวิธีการเข้ารหัสข้อมูลแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันนิติวิทยาศาสตร์
 - 4.1 ในกรณีที่ในตารางฐานข้อมูลเดียวกันมีฟิลด์ข้อมูลที่มีชั้นความลับและไม่มีชั้นความลับอยู่ร่วมกันให้ทำการเข้ารหัสข้อมูลเฉพาะฟิลด์ข้อมูลที่มีชั้นความลับเท่านั้น
 - 4.2 ในกรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บ ดังนี้
 - เก็บในสถานที่ที่เหมาะสม สามารถปิดล็อกได้เมื่อไม่ใช้งาน
 - เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร เป็นต้น โดยทันที เพื่อเป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิในการเข้าถึงข้อมูล เข้าถึงข้อมูลได้
5. กำหนดให้มีวิธีปฏิบัติการกู้คืนข้อมูลที่จัดเก็บถาวร สำหรับข้อมูลที่มีความสำคัญมากต่อการดำเนินงานของหน่วยงาน เพื่อสอบทานความถูกต้อง ครบถ้วน ความพร้อมใช้งาน คุณภาพข้อมูล

6. ในการจัดเก็บข้อมูลส่วนบุคคลให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และไม่เก็บรวบรวมข้อมูลส่วนบุคคลอันใด เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือกฎหมายอื่นบัญญัติให้กระทำได้ ดังนี้

- เชื้อชาติ
- เผ่าพันธุ์
- ความคิดเห็นทางการเมือง
- ความเชื่อในลัทธิ ศาสนาหรือปรัชญา
- พฤติกรรมทางเพศ
- ประวัติอาชญากรรม
- ข้อมูลสุขภาพ
- ความพิการ
- ข้อมูลสภาพแรงงาน
- ข้อมูลพันธุกรรม
- ข้อมูลชีวภาพ
- ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกัน

7. กำหนดให้มีการยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

8. ในกรณีที่มีการประชุมหรือธุรกรรมออนไลน์ กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ให้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์และในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้

- เก็บลงในสื่อที่รักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อได้
- มีการรักษาความลับของข้อมูล และกำหนดชั้นความลับในการเข้าถึงและจัดเก็บข้อมูล เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบแก้ไขข้อมูลที่จัดเก็บไว้ได้
- การจัดเก็บข้อมูลระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น Proxy Server NAT และอื่น ๆ

9. กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน

10. กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บถาวร เพื่อป้องกันข้อมูลไม่ให้เกิดการลบปรับปรุง แก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บถาวรรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต

11. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

12. ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของหน่วยงาน สำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่หน่วยงานจัดสรรไว้

13. กำหนดให้มีการทบทวนเกี่ยวกับช่วงระยะเวลาการจัดเก็บข้อมูล มาตรการ และวิธีปฏิบัติที่เกี่ยวข้องกับการจัดเก็บข้อมูลถาวร อย่างน้อยปีละ 1 ครั้ง

หมวด 3 การประมวลผลข้อมูลและการใช้ข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติในการประมวลผลข้อมูลและการใช้ข้อมูลที่มีประสิทธิภาพถูกต้อง ตรงตามวัตถุประสงค์ เพื่อให้เกิดประโยชน์สูงสุด

ผู้รับผิดชอบงาน

1. เจ้าของข้อมูล (Data Owners)
2. ผู้ใช้ข้อมูล (Data Users)
3. ผู้ดูแลระบบสารสนเทศ (System Administrators)

ข้อปฏิบัติ

1. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิเข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้
 - ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิการเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล
 - ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิเข้าถึงและใช้ข้อมูลตามอำนาจหน้าที่เท่านั้น
 - ข้อมูลใช้ภายใน กำหนดให้บุคลากรของสถาบันนิติวิทยาศาสตร์เท่านั้นที่มีสิทธิเข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้
2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการเข้าถึงข้อมูลในระบบเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด
3. เจ้าของข้อมูลจะต้องทบทวนสิทธิการเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ
4. ผู้ที่มีสิทธิเข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูลจะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ
5. ผู้ใช้ข้อมูลจะประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล
6. หน่วยงานต้องยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด
7. ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของสถาบันนิติวิทยาศาสตร์เพื่อประโยชน์เชิงธุรกิจเป็นการส่วนตัวหรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสมหรือใช้ข้อมูลอันก่อให้เกิดความเสียหายต่อสถาบันนิติวิทยาศาสตร์



หมวด 4 การเปิดเผยข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์และแนวปฏิบัติ ที่เกี่ยวข้อง ทั้งนี้ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนา ในรูปแบบต่าง ๆ ได้

ผู้รับผิดชอบงาน

1. เจ้าของข้อมูล (Data Owners)
2. ผู้ใช้ข้อมูล (Data Users)
3. บริกรข้อมูล (Data Stewards)
4. ทีมบริหารจัดการข้อมูล (Data Management Team)

ข้อปฏิบัติ

1. เจ้าของข้อมูลจะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ และมาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ

2. เจ้าของข้อมูลทำการเปิดเผยข้อมูลในความรับผิดชอบในรูปแบบข้อมูลเปิดของหน่วยงานโดยดำเนินการดังนี้

- กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
- กำหนดให้มีความอธิบายข้อมูลหรือเมทาดาทาสำหรับข้อมูลที่ต้องเปิดเผย
- ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน

- ข้อมูลที่เผยแพร่ต้องมาจากแหล่งที่เก็บข้อมูลโดยตรง ด้วยระดับความละเอียดสูงโดยไม่มีการปรับแต่งหรือเป็นข้อมูลรูปแบบสรุป (Summary data)

- ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย

3. กำหนดให้เงื่อนไขและข้อกำหนดของข้อมูลที่นำมาเปิดเผยภายในเครือข่ายของหน่วยงาน ข้อมูล ที่เผยแพร่ต้องไม่ขัดต่อกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง

4. สนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานและการลงทะเบียนบัญชีข้อมูลภาครัฐ โดยบริหารจัดการข้อมูลสำคัญ จัดทำบัญชีข้อมูลของหน่วยงาน และทำการลงทะเบียนบัญชีข้อมูลของหน่วยงานและ ชุดข้อมูลสำคัญ เข้าสู่ระบบบัญชีข้อมูลภาครัฐ (Government Data Catalog หรือ GD Catalog) เพื่อการเปิดเผย



ข้อมูลภาครัฐที่เป็นระบบ และมีเอกภาพ สามารถสืบค้นชุดข้อมูล คำอธิบายชุดข้อมูล รวมไปถึงแหล่งต้นทางของชุดข้อมูลภาครัฐที่สำคัญ สนับสนุนการใช้ประโยชน์ข้อมูลภาครัฐร่วมกัน

5. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และสนับสนุนการเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (Government Open Data) ผ่านเว็บไซต์ data.go.th โดย

- กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลที่กำหนดลำดับชั้นข้อมูล ตั้งแต่ลับขึ้นไป อย่างเพียงพอและมีประสิทธิภาพ

- มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าสถาบันนิติวิทยาศาสตร์ ได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า

- การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด

- หากการเปิดเผยนั้นเป็นการเปิดเผยบนช่องทางที่ดูแลรับผิดชอบโดยหน่วยงานอื่นที่ให้ปฏิบัติตามเอกสาร คู่มือ การนำข้อมูลขึ้นเผยแพร่ของหน่วยงานนั้น

- หากการเปิดเผยข้อมูลไม่ครบถ้วน หรือไม่ปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริการข้อมูลธุรกิจ บริการข้อมูลเทคนิค และทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

6. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

7. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงานรวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และ แนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงาน

8. กำหนดให้เจ้าของข้อมูลคัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูลที่มีคุณค่าสูง (High Value Dataset)

9. กำหนดให้เจ้าของข้อมูลต้องกำหนดกรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

หมวด 5 การทำลายข้อมูล

วัตถุประสงค์

กำหนดแนวปฏิบัติการทำลายข้อมูล และการพิจารณาอนุมัติทำลายโดยเจ้าของข้อมูลเพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

ผู้รับผิดชอบงาน

1. เจ้าของข้อมูล (Data Owners)
2. ผู้ทำลายข้อมูล (Data Destroyers)
3. ผู้ดูแลระบบสารสนเทศ (Systems Administrators)

ข้อปฏิบัติ

1. เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิในการทำลายข้อมูล และจะต้องทบทวนสิทธินั้น อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น
2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการทำลายข้อมูลในระบบให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด
3. ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน
4. กำหนดให้เจ้าของข้อมูลต้องจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาทาที่ทำลายสำหรับตรวจสอบในภายหลัง
5. กำหนดให้ผู้ทำลายข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี
6. กำหนดให้ผู้ใช้อข้อมูลส่วนบุคคลทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคล ร้องขอตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562



หมวด 6 การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

วัตถุประสงค์

เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล ทั้งภายในหน่วยงานและระหว่างหน่วยงาน อย่างมีประสิทธิภาพและก่อให้เกิดประโยชน์ต่อภาคประชาชน ภาครัฐ และภาคเอกชน

ผู้รับผิดชอบงาน

1. ผู้จัดการโครงการ (Project Managers)
2. ผู้ดูแลระบบแม่ข่าย (Server Administrators)
3. เจ้าของข้อมูล (Data Owners)
4. บริกรข้อมูล (Data Stewards)
5. ทีมบริหารจัดการข้อมูล (Data Management Team)

ข้อปฏิบัติ

1. กำหนดให้ผู้จัดการโครงการกำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการในความรับผิดชอบ ดังนี้
 - การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน กำหนดให้ใช้รูปแบบที่เป็นมาตรฐานเปิด (Open Format) ทั้งในส่วนมาตรฐานข้อมูล เช่น XML และ JSON เป็นต้น มาตรฐานโปรโตคอลสื่อสาร เช่น SOAP REST หรืออื่น ๆ ที่ได้รับการยอมรับจากมาตรฐานสากล
 - การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ให้ดำเนินการตามมาตรฐานกลางของหน่วยงานหลักที่เป็นผู้รับผิดชอบ
2. กำหนดให้ผู้จัดการโครงการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้
 - ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้
 - ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ นั่นคือ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว พร้อมทั้งตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ
 - หากไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริกรข้อมูลธุรกิจ บริกรข้อมูลเทคนิค และทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

3. ในกรณีที่มีหน่วยงานอื่นที่ไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูลส่วนบุคคลในการครอบครองของหน่วยงาน เพื่อการศึกษาหรือวิจัย ซึ่งเป็นข้อยกเว้นตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้หน่วยงานเจ้าของข้อมูลอนุญาตหน่วยงานนั้นในการเชื่อมโยงข้อมูลได้ โดยจะต้องแสดงข้อมูลนั้นด้วยวิธีไม่แสดงตัวตน (Anonymization)

4. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือ ข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต

5. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

6. กำหนดให้ผู้ดูแลระบบแม่ข่ายต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล เพื่อใช้ตรวจสอบสิ่งผิดปกติต่าง ๆ ที่เกิดขึ้นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล