



แนวปฏิบัติธรรมาภิบาลข้อมูลภาครัฐ และแผนงานการเปิดเผยข้อมูลภาครัฐ

สำนักงานคณะกรรมการป้องกัน
และปราบปรามการทุจริตในภาครัฐ
(สำนักงาน ป.ป.ท.)

นโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูลภาครัฐ

1. หลักการเหตุผล.....	1
2. นิยาม.....	1
3. ขอบเขต.....	3
4. แนวปฏิบัติ.....	3 - 14
วงจรชีวิตของข้อมูล.....	4
หมวดหมู่และการจัดระดับชั้นของข้อมูล.....	4
การเผยแพร่และการทบทวน.....	4
หมวด 1 การสร้างข้อมูล.....	5
หมวด 2 การจัดเก็บข้อมูล.....	7
หมวด 3 การประมวลผลข้อมูลและการใช้ข้อมูล.....	9
หมวด 4 การเชื่อมโยงและการแลกเปลี่ยนข้อมูล.....	10
หมวด 5 การเปิดเผยข้อมูล.....	11
หมวด 6 การทำลายข้อมูล.....	12
5. กระบวนการ.....	13
6. โครงสร้างของบุคลากรที่รับผิดชอบ.....	15
การควบคุมสิทธิ์การเข้าถึงข้อมูล (Access Control).....	18
แนวปฏิบัติสำหรับแบ่งปันและแลกเปลี่ยนข้อมูล (Shareable Data).....	19
กระบวนการตรวจสอบและประเมินคุณภาพข้อมูล (Data Quality).....	22
แผนงานการเปิดเผยข้อมูลภาครัฐ.....	23
กฎหมาย ระเบียบ ประกาศ ที่เกี่ยวข้อง.....	24

นโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูลภาครัฐ

1. หลักการเหตุผล

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ (สำนักงาน ป.ป.ท.) เป็นส่วนราชการในฝ่ายบริหารซึ่งรับผิดชอบเกี่ยวกับการป้องกันและปราบปรามการทุจริตในภาครัฐ ตามที่กำหนดในพระราชบัญญัติมาตรการของฝ่ายบริหารในการป้องกันและปราบปรามการทุจริต พ.ศ. 2551 และที่แก้ไขเพิ่มเติม และตามแนวนโยบายของรัฐบาล เป็นศูนย์กลางประสานงานกับหน่วยงานของรัฐที่เกี่ยวข้องทั้งหมด รวมทั้งกำหนดมาตรการต่างๆ เพื่อให้การป้องกันและปราบปรามการทุจริต ดำเนินการบูรณาการงาน ซึ่งในการดำเนินงานตามภารกิจต่างๆ นั้น มีข้อมูลที่เกี่ยวข้องเป็นทรัพย์สินสำคัญของสำนักงาน ป.ป.ท. จำเป็นต้องกำหนดสิทธิหน้าที่ และความรับผิดชอบ ของผู้มีส่วนได้ส่วนเสีย ในการบริหารจัดการข้อมูลทุกชั้นตอน เพื่อให้ได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคลและสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย ตามประกาศคณะกรรมการพัฒนาารัฐบาลดิจิทัล เรื่องธรรมาภิบาลข้อมูลภาครัฐ ประกาศ ณ วันที่ 12 มีนาคม พ.ศ. 2563 กำหนดให้หน่วยงานของรัฐดำเนินการให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ และจัดทำธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงานให้สอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้การบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวกรวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน

เพื่อให้สำนักงาน ป.ป.ท. ได้ดำเนินการบริหารจัดการข้อมูล ภาครัฐตามกฎหมาย ระเบียบและนโยบายธรรมาภิบาลของหน่วยงาน จึงได้จัดทำแนวปฏิบัติธรรมาภิบาลข้อมูลภาครัฐสำนักงาน ป.ป.ท. ฉบับนี้ขึ้น โดยมุ่งหวังให้เกิดการยกระดับให้ข้อมูลทั้งหมดของสำนักงาน ป.ป.ท. มีคุณภาพ มีความมั่นคงปลอดภัย มีความเป็นส่วนบุคคล และเป็นประโยชน์ต่อทุกภาคส่วน บนพื้นฐานของการคุ้มครองข้อมูลและรักษาผลประโยชน์ของประเทศและประชาชน และเพื่อใช้เป็นแนวทางในการดำเนินการที่สอดคล้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐ (DATA GOVERNANCE FRAMEWORK FOR GOVERNMENT) และถือเป็นภารกิจของคนทุกคนภายในองค์กรที่จะต้องร่วมมือกันดำเนินการตามธรรมาภิบาลที่ได้มีการกำหนดไว้ ซึ่งต้องทำอย่างต่อเนื่องสม่ำเสมอ จึงจะส่งผลให้ข้อมูลมีคุณภาพและขับเคลื่อนองค์กรด้วยข้อมูล (Data Driven Organization)

2. นิยาม

"ข้อมูล" หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าจะการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งนั้นบันทึกไว้ปรากฏได้

"ข้อมูลเปิด" หมายความว่า ข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้ แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มาหรือตามเจ้าของงานกำหนด

"ชุดข้อมูล" หมายความว่า การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะ โครงสร้างของข้อมูล

"บัญชีข้อมูล" หมายความว่า รายการของชุดข้อมูล ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภท ข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงานของรัฐ

"เมทาเดตา" หมายความว่า ข้อมูลที่ใช้อธิบายข้อมูล โดยระบุรายละเอียดแหล่งข้อมูล และคำอธิบาย รายละเอียดเกี่ยวกับข้อมูล ซึ่งจะทำให้ผู้ใช้ข้อมูลทราบว่าข้อมูลมาจากแหล่งใด มีรูปแบบอย่างไร ช่วยอำนวยความสะดวกในการสืบค้นข้อมูล

"คลังข้อมูล" หมายความว่า ระบบจัดการข้อมูลที่ได้จากการบูรณาการข้อมูลจากหลายแหล่งและใน หลายช่วงเวลา มีความสามารถในการเรียก/สืบค้น และรวบรวมข้อมูล ซึ่งข้อมูลที่เก็บรวบรวมบนคลังข้อมูลจะ อยู่ในรูปแบบข้อมูลที่มีโครงสร้าง โดยผ่านกระบวนการ Extract Transform Load (ETL) เพื่อให้อยู่ในรูปแบบ ที่เหมาะสมสำหรับการสร้าง Business Intelligence (BI) และการนำไปวิเคราะห์ข้อมูล

"ดาตาเลค" หมายความว่า แหล่งสำหรับเก็บรวบรวมข้อมูลที่มีหลากหลายรูปแบบ สามารถจัดเก็บ ข้อมูลที่มีโครงสร้าง ข้อมูลกึ่งโครงสร้าง และข้อมูลที่ไม่มีโครงสร้าง รวมไปถึงข้อมูลดิบที่ไม่มีการเปลี่ยนรูปแบบ ใดๆ โดยข้อมูลถูกเก็บรักษาไว้ในรูปแบบที่เหมือนหรือใกล้เคียงกับรูปแบบที่ได้รับมาจากแหล่งข้อมูลต้นฉบับ ใน การจัดการข้อมูลที่มีปริมาณมาก และหลากหลายรูปแบบ ทำให้เกิดความซับซ้อนในการใช้งานข้อมูลจึงต้อง อาศัยผู้เชี่ยวชาญในการจัดการ ได้แก่ Data Engineer เข้ามาช่วยดูแลระบบ, Data Analysis ทำหน้าที่ในการ วิเคราะห์ข้อมูล

"ดาตาอานาไลติกส์" หมายความว่า กระบวนการนำข้อมูลมาจัดการโดยการเรียงเรียง จัดระเบียบ แยก ประเภทชุดข้อมูล ตรวจสอบความถูกต้องของข้อมูล นำมาวิเคราะห์หาความสัมพันธ์ของข้อมูลในรูปแบบต่างๆ จนได้ข้อมูลเชิงลึก เพื่อสรุปหาสาเหตุ ช่วยสนับสนุนการตัดสินใจ หรือกำหนดนโยบายสำคัญขององค์กร

"ธรรมาภิบาลข้อมูลภาครัฐ" คือ การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการ บริหารจัดการข้อมูลภาครัฐทุกขั้นตอนเพื่อให้การได้มาและการนำข้อมูลของหน่วยงานของรัฐไปใช้อย่างถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนตัว และสามารถเชื่อมโยงแลกเปลี่ยน และบูรณาการระหว่างกัน ได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

"เจ้าหน้าที่ผู้มีหน้าที่ของสำนักงาน ป.ป.ท." หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ และพนักงานจ้างเหมาบริการ ซึ่งได้รับมอบหมายในการบริหารจัดการข้อมูลตามภารกิจ

"หน่วยงานที่แลกเปลี่ยนเชื่อมโยงข้อมูล" หมายความว่า หน่วยงานอื่น ๆ ที่ได้รับอนุญาตจากสำนักงาน ป.ป.ท. และมีความร่วมมือ หรือแนวทางในด้านการบริหารจัดการข้อมูลกับหน่วยงานนั้น ๆ อย่างชัดเจน

"บุคคลที่นำข้อมูลไปใช้" หมายความว่า เจ้าหน้าที่ของสำนักงาน ป.ป.ท. ทุกระดับ บุคคลภายนอก และ หน่วยงานภายนอกที่ได้รับสิทธิการเข้าถึงข้อมูล

"ความมั่นคงปลอดภัยของข้อมูล" หมายความว่า การดำเนินการตามหลักความมั่นคงปลอดภัยซึ่ง ประกอบด้วย ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน

(Availability) ของข้อมูล ทั้งนี้เพื่อป้องกันการสูญหายเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ

3. ขอบเขต

แนวปฏิบัติธรรมาภิบาลข้อมูลภาครัฐ สำนักงาน ป.ป.ท. นี้ ใช้กับเจ้าหน้าที่ผู้มีหน้าที่ของสำนักงาน ป.ป.ท. รวมทั้งหน่วยงานที่แลกเปลี่ยนเชื่อมโยงข้อมูลและบุคคลที่นำข้อมูลไปใช้

4. แนวปฏิบัติ

นโยบายและกรอบแนวทางปฏิบัติเพื่อเป็นหลักการในการบริหารจัดการข้อมูลภาครัฐของสำนักงาน ป.ป.ท. มีดังนี้

4.1 การเข้าถึงข้อมูล

การบริหารจัดการในการเข้าถึงข้อมูลกำหนดให้ผู้ใช้ข้อมูลต้องนำไปใช้อย่างเหมาะสมและสำนักงาน ป.ป.ท. จะปกป้องข้อมูลด้วยมาตรการรักษาความมั่นคงปลอดภัยที่ได้รับการรับรองตามมาตรฐานสากล

4.2 การนำข้อมูลไปใช้งานการสร้างความตระหนักรู้ของผู้ใช้ข้อมูล

รวมถึงความรับผิดชอบต่อผลของการนำข้อมูลไปใช้การเข้าถึงและใช้ข้อมูลตามความจำเป็นในการปฏิบัติงานโดยไม่แสวงหาผลประโยชน์ส่วนตัวหรือเพื่อวัตถุประสงค์อื่นที่ไม่เหมาะสม และใช้ข้อมูลให้เป็นไปตามระดับความปลอดภัยที่กำหนด

4.3 การบูรณาการข้อมูลกับหน่วยงานอื่น

สำนักงาน ป.ป.ท. มีการบูรณาการข้อมูลกับหน่วยงานอื่น โดยการจัดส่งข้อมูลเอกสารหรือการเชื่อมโยงข้อมูลผ่านระบบ โดยใช้ข้อมูลเลขประจำตัวประชาชน 13 หลัก หรือ ชื่อ สกุล เป็นเงื่อนไขหลักในการเชื่อมโยง หรือ ตามมาตรฐานการแลกเปลี่ยนข้อมูลระหว่างระบบสารสนเทศอิเล็กทรอนิกส์ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือตามมาตรฐานที่มติคณะรัฐมนตรีกำหนด หรือมีการตกลงเป็นลายลักษณ์อักษรเพื่อการเชื่อมโยงข้อมูลระหว่างหน่วยงาน โดยระบบจะทำการประมวลผลและตอบผลข้อมูลรายละเอียดตามแต่ละบริการ

4.4 การเก็บรักษาข้อมูล

สำนักงาน ป.ป.ท. ไม่มีหน้าที่ในการจัดเก็บข้อมูลของหน่วยงานที่แลกเปลี่ยนเชื่อมโยงข้อมูล แต่จะทำการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลการใช้งานของผู้ใช้ข้อมูลที่สอดคล้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และที่แก้ไขเพิ่มเติม

4.5 การเปิดเผยข้อมูล

ข้อมูลของสำนักงาน ป.ป.ท. ที่เปิดเผยให้เป็นไปตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ โดยต้องให้ประชาชนทั่วไปสามารถเข้าถึงได้อย่างเสรีโดยไม่เสียค่าใช้จ่าย และสามารถนำไปเผยแพร่ใช้ประโยชน์ หรือพัฒนาบริหารและนวัตกรรม ในรูปแบบต่าง ๆ ได้ เพื่อประโยชน์ในการอำนวยความสะดวกแก่ประชาชนในการเข้าถึงข้อมูล ทั้งนี้ ให้เป็นไปตามมาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลที่คณะกรรมการพัฒนารัฐบาลดิจิทัลกำหนด

4.6 การเผยแพร่และการทบทวน

สำนักงาน ป.ป.ท. อาจพิจารณาทบทวนหรือแก้ไขปรับปรุงแนวปฏิบัติฉบับนี้เพื่อให้สอดคล้องกับกฎหมาย ระเบียบ หรือนโยบายที่เกี่ยวข้อง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

วงจรชีวิตของข้อมูล

วงจรชีวิตของข้อมูล หรือระบบบริหารและกระบวนการจัดการข้อมูล หมายถึงลำดับขั้นตอนของข้อมูล ตั้งแต่ เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ประกอบด้วย กระบวนการสร้างข้อมูล (Create) กระบวนการจัดเก็บข้อมูล (Store) กระบวนการใช้ข้อมูล (Use) กระบวนการเผยแพร่ข้อมูล (Publish) กระบวนการจัดเก็บข้อมูลถาวร (Archive) และกระบวนการทำลายข้อมูล (Destroy)

หมวดหมู่และการจัดระดับชั้นของข้อมูล

ข้อมูลของหน่วยงานสามารถแบ่งหมวดหมู่ตามกรอบธรรมาภิบาลข้อมูลและการทำงานของสำนักงาน ป.ป.ท. ได้ดังนี้

- ข้อมูลที่มีชั้นความลับ (Secret) แบ่งเป็น ข้อมูลลับที่สุด (Top Secret) ข้อมูลลับมาก (Secret) และข้อมูลลับ (Confidential)
- ข้อมูลภายในองค์กร (Internal Use) ได้แก่ ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงาน ซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต
- ข้อมูลสาธารณะ และข้อมูลเปิดเผยได้ (Public) ได้แก่ ข้อมูลที่สามารถเปิดเผยบุคคลทั่วไป โดยไม่ก่อให้เกิดความเสียหาย

การเผยแพร่และการทบทวน

แนวปฏิบัติการดำเนินงานด้านธรรมาภิบาลข้อมูลนี้จะต้องทำการเผยแพร่โดยการประกาศในเว็บไซต์สำนักงาน ป.ป.ท. เพื่อให้เจ้าหน้าที่รับทราบ และถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด ซึ่งแนวปฏิบัตินี้จะต้องถูกทบทวนอย่างน้อยปีละ 1 ครั้ง รวมถึงเมื่อมีข้อเสนอแนะจากคณะกรรมการข้อมูลข่าวสารและเปิดเผยข้อมูลภาครัฐ ของสำนักงาน ป.ป.ท.

หมวด 1 การสร้างข้อมูล

กระบวนการสร้างข้อมูล เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติ ด้วยอุปกรณ์อิเล็กทรอนิกส์ รวมถึงการซื้อข้อมูล หรือการรับข้อมูลมาจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง

กิจกรรม	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล	✓		
กำหนดชั้นความลับข้อมูลของข้อมูลที่ถูกสร้างขึ้น	✓		
กำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูล			✓
จัดทำคำอธิบายชุดข้อมูลดิจิทัล	✓	✓	
ประเมินคุณค่าของชุดข้อมูลดิจิทัล	✓	✓	
ตรวจสอบความถูกต้องของข้อมูล	✓		

1. เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล และจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

2. เจ้าของข้อมูลเป็นผู้กำหนดชั้นความลับของข้อมูลที่ถูกสร้างขึ้นตามวิธีปฏิบัติการจำแนกชั้นความลับของข้อมูล

3. เจ้าของข้อมูลกำหนดให้มีวิธีปฏิบัติการจำแนกชั้นความลับข้อมูลสำหรับข้อมูลที่ถูกสร้างขึ้น

4. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด

5. เจ้าของข้อมูลร่วมกับบริการข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานคำอธิบายชุดข้อมูลดิจิทัลที่สำนักงาน ป.ป.ท. กำหนด และสอดคล้องกับมาตรฐานที่ภาครัฐได้กำหนดไว้

6. เจ้าของข้อมูลร่วมกับบริการข้อมูลทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมินคุณค่าชุดข้อมูลที่ สพร. หรือสำนักงาน ป.ป.ท. กำหนดและเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล

7. ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะดังต่อไปนี้ เข้าสู่ระบบคอมพิวเตอร์ที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

- ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลอันเป็นเท็จ ซึ่งจะเกิดความเสียหายแก่ประชาชน
- ข้อมูลอันเป็นเท็จที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัย สาธารณะ ความมั่นคงทางเศรษฐกิจ หรือโครงสร้างพื้นฐาน หรือก่อให้เกิดความตื่นตระหนก
- ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือความผิดเกี่ยวกับการก่อการร้าย
- ข้อมูลที่มีลักษณะอันลามก และประชาชนทั่วไปอาจเข้าถึงได้
- ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทาง อิเล็กทรอนิกส์หรือวิธีการอื่นใดทำให้ผู้อื่นเสียชื่อเสียง

8. ห้ามมิให้ผู้สร้างข้อมูลทำการสร้าง ทำซ้ำหรือดัดแปลงต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่นเว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง

9. กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น

10. กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกรสร้างขึ้น

11. กำหนดให้มีวิธีปฏิบัติเกี่ยวกับสร้างข้อมูลให้มีความปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

หมวด 2 การจัดเก็บข้อมูล

กระบวนการจัดเก็บข้อมูล เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือข้อมูลที่ได้จากการแลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลาย และให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว

กิจกรรม	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดระยะเวลาในการจัดเก็บข้อมูล	✓		
ตรวจสอบความครบถ้วนของชุดข้อมูลหรือเมทาดาตาของการจัดเก็บชุดข้อมูล	✓	✓	
ทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดเพื่อจัดเก็บเป็นข้อมูลถาวร	✓	✓	
จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์			✓

1. เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน
2. กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูลและบริการข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน
3. บริการข้อมูลและผู้ดูแลระบบสารสนเทศ ทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้ว เพื่อจัดเก็บเป็นข้อมูลถาวร
4. การจัดเก็บข้อมูลที่มีชั้นความลับให้ทำการเข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
5. กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ เพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์
6. กำหนดให้การจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้
 - เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อดังกล่าวได้
 - มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้

- การจัดเก็บข้อมูลต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้ (Identification and Authentication)
7. กรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บดังนี้
- เก็บในสถานที่ที่มีมาตรการป้องกันการเข้าถึงข้อมูล เช่น สามารถปิดล็อกได้เมื่อไม่ใช้งาน
 - เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ ได้แก่ เครื่องถ่ายเอกสาร เครื่องพิมพ์ เป็นต้น เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์ในการเข้าถึงข้อมูลได้
8. กำหนดให้มีการจัดเก็บข้อมูลส่วนบุคคล โดยให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
9. กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน
10. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ
11. ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของสำนักงาน สำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่สำนักงานจัดสรรไว้

หมวด 3 การประมวลผลข้อมูลและการใช้ข้อมูล

กระบวนการใช้ข้อมูล (Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน รวมถึงการสำรอง (Backup) ข้อมูล เพื่อเป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

กิจกรรม	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดสิทธิ์ประมวลผลและเข้าใช้งานข้อมูลตามชั้นความลับ	✓		
กำหนดสิทธิ์ในการประมวลผลและเข้าใช้งานข้อมูลให้แก่ผู้ใช้ข้อมูล			✓
ทบทวนสิทธิ์การเข้าถึงและการใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง	✓		

1. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้
 - ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิ์ตามตำแหน่ง/บทบาท เท่านั้น
 - ข้อมูลใช้ภายใน กำหนดให้ผู้บริหาร ข้าราชการ ลูกจ้าง และเจ้าหน้าที่ของรัฐเท่านั้น ที่มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้ ทั้งนี้ ต้องปกป้องข้อมูลจากการเข้าถึงโดยบุคคลภายนอก
 - ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล
2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการเข้าถึงเพื่อประมวลผล และใช้ข้อมูลผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด
3. เจ้าของข้อมูลจะต้องทบทวนสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ
4. ผู้ที่มีสิทธิ์เข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูลจะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ
5. ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของหน่วยงาน เพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสม หรือใช้ข้อมูลอันก่อให้เกิดความเสียหายต่อหน่วยงาน

หมวด 4 การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลทั้งภายในหน่วยงานและระหว่างหน่วยงานอย่างมีประสิทธิภาพ และก่อให้เกิดประโยชน์ต่อภาครัฐ ภาคเอกชน และประชาชน โดยเป็นการเชื่อมโยงและแลกเปลี่ยนข้อมูล ให้มีความมั่นคงปลอดภัย น่าเชื่อถือ และข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

กิจกรรม	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดแนวทาง/กระบวนการ ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล	✓	✓	
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา และตรวจสอบชั้นความลับของข้อมูล	✓	✓	✓
กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล			✓
กำหนดมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล	✓	✓	
จัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล (Log File)			✓
ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำไปใช้	✓	✓	

1. กำหนดให้เจ้าของข้อมูลหรือบริการข้อมูล จัดทำแนวทาง/กระบวนการ ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล
2. กำหนดให้เจ้าของข้อมูล หรือบริการข้อมูลตามที่ได้รับมอบหมายดำเนินการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาของข้อมูลที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน
3. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล
4. บริการข้อมูลร่วมกับผู้ดูแลระบบสารสนเทศ กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต
5. กำหนดให้ผู้ดูแลระบบสารสนเทศต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยง และการแลกเปลี่ยนข้อมูลดิจิทัล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

6. บริการข้อมูลร่วมกับผู้ดูแลระบบสารสนเทศ ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำไปใช้

7. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูล ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

หมวด 5 การเผยแพร่และการเปิดเผยข้อมูล

เพื่อกำหนดแนวปฏิบัติและมาตรฐานการเผยแพร่และการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนาในรูปแบบต่าง ๆ ได้

กิจกรรม	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ง่าย	✓	✓	
คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด (Open Data)	✓	✓	
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาทาของชุดข้อมูลที่จะทำการเปิดเผยให้มีความครบถ้วนเป็นปัจจุบัน	✓	✓	
กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย	✓	✓	

1. เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ง่าย
2. กำหนดให้เจ้าของข้อมูลร่วมกับบริการข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูล
3. เจ้าของข้อมูลร่วมกับบริการข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด (Open Data) ในรูปแบบข้อมูลเปิดของสำนักงาน ป.ป.ท.
4. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และต้องเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (data.go.th) และระบบบัญชีภาครัฐ (gdcatalog.go.th)
5. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
6. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคง และข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงาน ยกเว้นได้รับการอนุมัติจากสำนักงาน ป.ป.ท. รวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงานเจ้าของข้อมูล

หมวด 6 การทำลายข้อมูล

เพื่อกำหนดแนวปฏิบัติการทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

กิจกรรม	เจ้าของข้อมูล	บริการข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้ทำลาย
กำหนดผู้มีสิทธิในการทำลายข้อมูล	✓	✓		
กำหนดสิทธิในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูล			✓	
ทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน				✓
จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาทาที่ทำลายสำหรับตรวจสอบในภายหลัง	✓	✓		
จัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี				✓
ทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอหรือข้อมูลส่วนบุคคลที่พ้นระยะเวลาการเก็บรักษา ตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล				✓

1. เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดผู้มีสิทธิในการทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และจะต้องทบทวนสิทธินั้นอย่างน้อยปีละ 1 ครั้ง
2. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด
3. ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ป.ป.ท.
4. กำหนดให้เจ้าของข้อมูลร่วมกับบริการข้อมูล จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาทาที่ทำลาย สำหรับตรวจสอบในภายหลัง

5. กำหนดให้ผู้ทำลายข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยเก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี

6. กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยจะต้องผ่านการเห็นชอบจากผู้ควบคุมข้อมูลส่วนบุคคลและดำเนินการตามข้อกำหนดที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนดไว้อย่างเคร่งครัด

5. กระบวนการ

ขั้นตอนที่ใช้สำหรับกำกับ ดูแลการดำเนินการใด ๆ ต่อข้อมูลให้เป็นไปตามกฎหมาย ระเบียบ หรือ นโยบายที่เกี่ยวข้องกับข้อมูลมีรายละเอียดและแนวปฏิบัติ ดังต่อไปนี้

5.1 การสร้างข้อมูล

5.1.1. การสร้างและการรวบรวมข้อมูล มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลโดยปฏิบัติตามแนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคล และแนวปฏิบัติในด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสำนักงาน ป.ป.ท. ทั้งนี้ ให้เป็นไปตามที่กฎหมายกำหนด

5.1.2. จัดชั้นความลับของข้อมูลที่จะเก็บรวบรวม ใช้ หรือเปิดเผย

5.1.3. จัดให้มีคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐและบัญชีข้อมูลจากข้อมูลต่าง ๆ ที่รวบรวมให้มีความถูกต้อง ครบถ้วนและเป็นปัจจุบัน

5.2 การจัดเก็บข้อมูลและการทำลายข้อมูล

5.2.1. การเก็บข้อมูล สำนักงาน ป.ป.ท. จะใช้วิธีตามที่กฎหมายกำหนดในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล โดยสำนักงาน ป.ป.ท. จะเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัดและเท่าที่จำเป็น ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล

5.2.2. การจัดเก็บ การจัดเก็บถาวร ต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและความเป็นส่วนบุคคลของข้อมูล ให้เป็นไปตามที่กฎหมายกำหนด หรือแนวปฏิบัติในการปกป้องข้อมูล หรือแนวปฏิบัติในด้านความมั่นคงปลอดภัยและชั้นความลับของข้อมูล

5.2.3. การจัดเก็บข้อมูล ต้องจัดเก็บลงในสื่อบันทึกข้อมูลและมีโครงสร้างข้อมูลตามมาตรฐานสถาปัตยกรรมข้อมูล ข้อมูลหลัก และข้อมูลอ้างอิง

5.2.4. การจัดเก็บถาวร ต้องเป็นการดำเนินการกับข้อมูลที่ไม่มีการลบ ปรับปรุง หรือแก้ไขอีกต่อไปและสามารถนำกลับมาใช้งานได้ โดยให้เป็นไปตามที่กฎหมายกำหนด

5.2.5. การจัดเก็บข้อมูลชั้นความลับที่เป็นข้อมูลความลับทางราชการ และข้อมูลความมั่นคงต้องมีการเข้ารหัสข้อมูล

5.2.6. การสำรองข้อมูล ต้องจัดเก็บให้มีความถูกต้องครบถ้วนเป็นปัจจุบัน ตามมาตรฐานการสำรองข้อมูล

5.2.7. การทำลายข้อมูล ต้องเป็นการดำเนินการกับข้อมูลที่ไม่ต้องนำกลับมาใช้งานได้อีกต่อไปโดยให้เป็นไปตามที่กฎหมายกำหนด

5.3 การประมวลผลข้อมูลและการใช้ข้อมูล

- 5.3.1. สิทธิการประมวลผลข้อมูลและการใช้งานของผู้ใช้ข้อมูล ให้เป็นตามวัตถุประสงค์ของการใช้งานและคำนึงถึงขั้นความลับของข้อมูล โดยให้เป็นไปตามที่กฎหมายกำหนด
- 5.3.2. การประมวลผลข้อมูลและการใช้ข้อมูลต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามแนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคล และแนวปฏิบัติในด้านความมั่นคงปลอดภัยและความเป็นส่วนตัวของข้อมูล โดยให้เป็นไปตามที่กฎหมายกำหนด
- 5.3.3. การประมวลผลและการใช้ข้อมูล ต้องมีความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องการ (Consistency) ความเป็นปัจจุบัน (Timeliness) และมีคุณภาพ (Quality)
- 5.3.4. การเรียกใช้ข้อมูลชั้นความลับที่เป็นข้อมูลความลับทางราชการ และข้อมูลความมั่นคงต้องมีการกำหนดสิทธิการเข้าใช้ข้อมูลและข้อมูลความมั่นคงต้องมีการกำหนดสิทธิการเข้าใช้ข้อมูล
- 5.3.5. ต้องจัดให้มีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล เพื่อให้สามารถตรวจสอบย้อนกลับได้ โดยให้เป็นไปตามที่กฎหมายกำหนด
- 5.3.6. ผู้ใช้ข้อมูลจะต้องเป็นผู้รับผิดชอบหากมีการประมวลผลข้อมูลและการใช้ข้อมูลที่ไม่เป็นไปตามที่กฎหมายกำหนด

5.4 การเปิดเผยข้อมูล

- 5.4.1. การเปิดเผยข้อมูลต่าง ๆ จะต้องเป็นไปตามที่กฎหมายกำหนด
- 5.4.2. สำนักงาน ป.ป.ท. จะเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลในกรณีใดกรณีหนึ่ง ดังต่อไปนี้
 - ได้รับความยินยอมจากเจ้าของข้อมูล
 - เป็นความจำเป็นเพื่อการปฏิบัติงานของราชการหรือตามคำขอของเจ้าของข้อมูล
 - เป็นความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย
 - เป็นการปฏิบัติงานตามกฎหมายหรือกฎเกณฑ์ของทางราชการหรือคำสั่งของหน่วยงานที่มีอำนาจกำกับดูแล หรือที่มีอำนาจตามกฎหมาย
- 5.4.3. การเผยแพร่ข้อมูลหรือการเปิดเผยข้อมูลในรูปแบบดิจิทัล ต้องปฏิบัติตามแนวทางการเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบดิจิทัลต่อสาธารณะของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

5.5 การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

- 5.5.1. การเชื่อมโยงและการแลกเปลี่ยนข้อมูลของสำนักงาน ป.ป.ท. กับหน่วยงานอื่น ๆ จะต้องได้รับอนุญาตจากสำนักงาน ป.ป.ท. และมีความร่วมมือ หรือแนวทางในด้านการบริหารจัดการข้อมูลกับหน่วยงานนั้น ๆ อย่างชัดเจน
- 5.5.2. การเชื่อมโยงและการแลกเปลี่ยนข้อมูล ต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามแนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคล และแนวปฏิบัติในด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยให้เป็นไปตามที่กฎหมายกำหนด
- 5.5.3. เทคโนโลยีและวิธีการทางเทคนิคที่เกี่ยวข้องกับการเชื่อมโยงและการแลกเปลี่ยนข้อมูลให้เป็นไปตามมาตรฐานสากล

5.6 การติดตามและประเมินผลการใช้งานข้อมูล

สำนักงาน ป.ป.ท. จะกำหนดให้มีการติดตามและประเมินผลการใช้งานข้อมูลอย่างน้อยปีละ 1 ครั้ง โดยจัดทำเป็นรายงานเสนอไปยังผู้บริหาร

6. โครงสร้างของบุคลากรที่รับผิดชอบ

6.1 หัวหน้าหน่วยงาน (Chief Executive Officer : CEO)

ผู้รับผิดชอบ: เลขาธิการคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

มีหน้าที่: ตัดสินใจเชิงนโยบายแก้ไขปัญหา บริหารจัดการและสนับสนุนธรรมาภิบาลข้อมูลภายในหน่วยงาน

6.2 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer : DCIO)

ผู้รับผิดชอบ: ผู้บริหารระดับสูงที่ได้รับมอบหมายให้กำกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

มีหน้าที่: ให้ข้อเสนอแนะ และอนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติงาน เกณฑ์การวัดคุณภาพ ระเบียบ และข้อบังคับอื่น ๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการบริหารจัดการ การจัดลำดับความสำคัญ และแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล

6.3 คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee)

ผู้รับผิดชอบ: คณะกรรมการดิจิทัล สำนักงาน ป.ป.ท. ประกอบด้วย ผู้บริหารจากสำนัก กอง และศูนย์ฯ

มีหน้าที่: ให้คำปรึกษา กำกับดูแลข้อมูล พร้อมเสนอแนะนโยบายและแนวทางการบริหารจัดการข้อมูล

6.4 ผู้บริหารข้อมูลระดับสูง (Chief Data Officer : CDO)

ผู้รับผิดชอบ: ผู้บริหารที่ได้รับมอบหมาย

มีหน้าที่: ให้ข้อเสนอแนะ และอนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติงาน เกณฑ์การวัดคุณภาพ ระเบียบ และข้อบังคับอื่น ๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการบริหารจัดการ การจัดลำดับความสำคัญ และแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล

6.5 เจ้าของข้อมูล (Data Owner)

ผู้รับผิดชอบ: หัวหน้าหน่วยงานผู้มีหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง

มีหน้าที่: รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือ กฎหมาย เจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลง Metadata และเกณฑ์การทำ Data Cleansing รวมถึงการกำหนดสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

6.6 ทีมบริการข้อมูล (Data Stewards Team)

ผู้รับผิดชอบ ประกอบด้วย หัวหน้าบริการข้อมูล (Lead Data Steward) บริการข้อมูลด้านธุรกิจ บริการข้อมูลด้านเทคนิค บริการข้อมูลด้านคุณภาพข้อมูล รวมไปถึงบุคคลที่ทำหน้าที่เกี่ยวกับความมั่นคงปลอดภัย กฎหมาย และบุคคลที่ให้ความรู้เกี่ยวกับนโยบายข้อมูลและความรู้อื่น ๆ มีหน้าที่: ต้องดำเนินการดังนี้

- กำหนด ทบทวนความต้องการด้านคุณภาพข้อมูล การรักษาความเป็นส่วนตัว และความมั่นคงปลอดภัยของข้อมูล
- กำหนด ทบทวน และปรับปรุงกระบวนการให้สอดคล้องกับนโยบายข้อมูล เป้าประสงค์ ความต้องการของผู้มีส่วนได้เสียกับข้อมูล รวมทั้งติดตามการดำเนินงานตามแผนที่กำหนดเพื่อนำมาปรับปรุงกระบวนการทำงาน
- กำหนดนิยามคำอธิบายชุดข้อมูลดิจิทัล พร้อมทั้งจัดทำบัญชีข้อมูลให้ครบถ้วนตามความจำเป็นในการใช้งาน และตรงตามความต้องการของผู้มีส่วนได้เสียกับข้อมูล
- วิเคราะห์ความพร้อมของธรรมาภิบาลข้อมูล ความต้องการด้านคุณภาพข้อมูล การรักษาความเป็นส่วนตัว และความมั่นคงปลอดภัยให้เหมาะสมกับสถานการณ์ปัจจุบัน เพื่อวางแผนการวัดและประเมินผล
- ตรวจสอบ วิเคราะห์ วัดผลการดำเนินงาน
- ให้ข้อเสนอแนะเชิงเทคนิคที่สอดคล้องกับนโยบาย เป้าประสงค์ และความต้องการของผู้มีส่วนได้เสียกับข้อมูล
- กำหนดรายละเอียดที่เกี่ยวข้องกับการออกแบบระบบเทคโนโลยีสารสนเทศ รวมถึงโครงสร้างพื้นฐาน เทคโนโลยีสารสนเทศ เพื่อคุ้มครองข้อมูลส่วนบุคคล และรักษาความมั่นคงปลอดภัย
- สนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศและอื่น ๆ ที่เกี่ยวข้อง
- รายงานผลลัพธ์ไปยังคณะกรรมการดิจิทัล สำนักงาน ป.ป.ท. และผู้เกี่ยวข้อง

6.7 ทีมบริหารจัดการข้อมูล (Data Management Team)

ผู้รับผิดชอบ: ประกอบด้วย เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และเจ้าหน้าที่ที่ได้รับมอบหมายของหน่วยงาน

มีหน้าที่: ต้องดำเนินการบริหารจัดการข้อมูล ตามองค์ประกอบดังนี้

- สถาปัตยกรรมข้อมูล (Data Architecture)
- การจำลองและการออกแบบข้อมูล (Data Modeling and Design)
- การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operation)
- การบูรณาการและความสามารถในการทำงานร่วมกัน (Data Integration and Interoperability)
- การบริหารจัดการเอกสารและเนื้อหา (Document and Content Management)
- ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data)
- คลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอานาไลติกส์

- คำอธิบายชุดข้อมูลดิจิทัล หรือ Metadata
- ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนตัวของข้อมูล (Data Security and Privacy)
- คุณภาพของข้อมูล (Data Quality)

6.8 ผู้สร้างข้อมูล (Data Creators)

ผู้รับผิดชอบ: เจ้าหน้าที่ของหน่วยงานที่เป็นเจ้าของข้อมูล

มีหน้าที่: บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ ถูกกำหนดไว้ รวมถึงทำงานร่วมกับทีมบริการข้อมูล เพื่อตรวจสอบ แก้ไขด้านคุณภาพ และความมั่นคงปลอดภัยข้อมูล

6.9 ผู้ใช้ข้อมูล (Data Users)

ผู้รับผิดชอบ ประกอบด้วย เจ้าหน้าที่ของสำนักงาน ป.ป.ท. ทุกระดับ บุคคลภายนอก และหน่วยงานภายนอกที่ได้รับสิทธิการเข้าถึงข้อมูล

มีหน้าที่: นำข้อมูลไปใช้งาน ต้องสนับสนุนธรรมาภิบาลข้อมูลภาครัฐ โดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้อข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูล ไปยังทีมบริการข้อมูล

การควบคุมสิทธิ์การเข้าถึงข้อมูล (Access Control)

สำนักงาน ป.ป.ท. ได้กำหนดแนวทางการควบคุมสิทธิ์การเข้าถึงข้อมูลของหน่วยงาน เพื่อให้การบริหารจัดการข้อมูลเป็นไปอย่างมีประสิทธิภาพ โดยมีรายละเอียด ดังนี้

1. การเข้าถึงข้อมูลผ่านระบบสารสนเทศ

1. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล ตามความจำเป็นต่อการใช้งาน เท่านั้น

2. บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูง หรือหัวหน้าหน่วยงานแล้วแต่กรณี เพื่อให้ความเห็นชอบและอนุญาตก่อน

3. ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ โดยผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิ์ตามอนุญาตนั้น ดังนี้

3.1 กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้: อ่านอย่างเดียว / สร้างข้อมูล / ป้อนข้อมูล / แก้ไข / อนุมัติ / ไม่มีสิทธิ์

3.2 กำหนดเกณฑ์การระงับสิทธิ์มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

3.3 ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศและปฏิบัติงานตามหัวหน้าหน่วยงานมอบหมาย: อนุญาตให้ผู้ใช้งานเข้าถึงระบบ / กำหนดสิทธิ์และทบทวนสิทธิ์อย่างสม่ำเสมอ / ติดตั้งระบบบันทึกและติดตามการใช้งาน

4. จัดแบ่งประเภทของข้อมูล ชั้นความลับ ตามมาตรฐาน นโยบายแนวปฏิบัติที่สำนักงาน ป.ป.ท. กำหนด รวมถึงระดับชั้นการเข้าถึง เวลาเข้าถึง และช่องทางการเข้าถึงข้อมูลไว้ให้ชัดเจน โดยจัดแบ่งระดับชั้นการเข้าถึงอย่างน้อย ดังนี้

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

5. เจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ ยังคงมีความเหมาะสม

6. ระบบงานสารสนเทศที่มีการเชื่อมโยงข้อมูลกันให้อำนาจการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารพิจารณาประเด็น ต่าง ๆ ทางด้านความมั่นคงปลอดภัย ก่อนตัดสินใจใช้ข้อมูลร่วมกัน โดยมีประเด็นต้องดำเนินการอย่างน้อย ดังนี้

- 6.1 กำหนดนโยบายและมาตรการเพื่อควบคุมดูแล และบริหารจัดการการใช้ข้อมูลร่วมกัน
- 6.2 พิจารณาจำกัดหรือการอนุญาตการเข้าถึงข้อมูลส่วนบุคคล
- 6.3 พิจารณาว่ามีบุคคล กลุ่มบุคคล ที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

6.4 พิจารณาเกี่ยวกับระบบการลงทะเบียนและบริหารสิทธิ์ผู้ใช้งาน

6.5 ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

แนวปฏิบัติสำหรับแบ่งปันและแลกเปลี่ยนข้อมูล (Shareable Data)

สำนักงาน ป.ป.ท. กำหนดแนวปฏิบัติสำหรับแบ่งปันและแลกเปลี่ยนข้อมูล (Shareable Data) ทั้งภายในหน่วยงานและระหว่างหน่วยงาน เพื่อมีประสิทธิภาพ และประโยชน์ต่อการแลกเปลี่ยนข้อมูลภายในหน่วยงาน ภาคประชาชน และหน่วยงานภาครัฐ

ผู้รับผิดชอบ

- เจ้าของข้อมูล (Data Owners)
- คณะบริการข้อมูล (Data Stewards)
- ผู้ดูแลระบบ (System Administrators)
- ผู้จัดการโครงการ (Project Managers)
- ทีมบริหารจัดการข้อมูล (Data Management Team)

กระบวนการขั้นตอนการปฏิบัติงาน

1. กำหนดให้ผู้จัดการโครงการกำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการในความรับผิดชอบ ดังนี้
 - 1.1 การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน กำหนดให้ใช้รูปแบบที่เป็นมาตรฐานเปิด (Open Format) ทั้งในส่วนมาตรฐานข้อมูล เช่น XML และ JSON เป็นต้น มาตรฐานโปรโตคอลสื่อสาร เช่น SOAP REST หรืออื่น ๆ ที่ได้รับการยอมรับจากมาตรฐานสากล
 - 1.2 การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ให้ดำเนินการตามมาตรฐานกลางของหน่วยงานหลักที่เป็นผู้รับผิดชอบ
2. กำหนดให้ผู้จัดการโครงการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาทาที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน
 - 2.1 ตรวจสอบเมทาดาทาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้
 - 2.2 ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่
 - 2.3 หากไม่ครบถ้วน หรือไม่ปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริการข้อมูลธุรกิจ บริการข้อมูลเทคนิค และทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน
3. ในกรณีที่มิหน่วยงานอื่นที่ไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูลส่วนบุคคล เพื่อทำการศึกษาหรือวิจัย ซึ่งเป็นข้อยกเว้นตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้หน่วยงาน

เจ้าของข้อมูลอนุญาตหน่วยงานนั้นในการเชื่อมโยงข้อมูลได้ โดยจะต้องแสดงข้อมูลนั้นด้วยวิธีไม่แสดงตัวตน (Anonymization)

4. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลเพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต
5. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์
6. กำหนดให้ผู้ดูแลระบบแม่ข่ายต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลเพื่อใช้ตรวจสอบสิ่งผิดปกติต่างๆ ที่เกิดขึ้น

มาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูล

สำนักงาน ป.ป.ท. มีแนวทางการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลทั้งภายในหน่วยงานและระหว่างหน่วยงาน รายละเอียดดังตารางต่อไปนี้

หมวดมาตรฐาน	คำอธิบาย	ตัวอย่าง
มาตรฐานการเชื่อมโยง (Interconnection Specification)	รายการมาตรฐานที่ใช้ในการเชื่อมโยงระบบข้อมูล รวมถึงระบุแนวทางการเชื่อมโยงในระดับโปรโตคอลมาตรฐานต่างๆ	HTTP, SMTP, POP3, IMAP, FTP, SMS
มาตรฐานการแลกเปลี่ยนข้อมูล (Data Exchange Specification)	รายการมาตรฐานเพื่อการแลกเปลี่ยนข้อมูลครอบคลุมถึงเทคโนโลยีและมาตรฐานต่างๆ สำหรับการจัดโครงสร้างข้อมูล (Structure) และการเข้ารหัสข้อมูล (Encode)	XML: Extensible Markup Language
มาตรฐานรูปแบบการจัดเก็บและนำเสนอข้อมูล (Storage & Presentation Specification)	มาตรฐานและเทคโนโลยีที่เกี่ยวข้องกับการนำเสนอสารสนเทศ ช่วยให้สารสนเทศสามารถถูกนำมาแสดงผลได้ในรูปแบบที่สอดคล้องกัน	XML Schema, RSS, XLS/XLSX, CSV, E-R Diagram
บริการผ่านเว็บเซอร์วิสเทคโนโลยี (Web Technology Specification)	มาตรฐานและเทคโนโลยีที่เกี่ยวข้องกับการแลกเปลี่ยนข้อมูลระหว่างระบบที่มีแพลตฟอร์มเหมือนกันและแตกต่างกัน	SOAP, UDDI, WSDL
บริการด้านธุรกรรม (Business Service Specification)	มาตรฐานและเทคโนโลยีในกลุ่มงานธุรกรรมที่มีเทคนิคเฉพาะด้านของกลุ่มงานนั้น	ebXML, ebRIM, ebRS, ebMS

หมวดมาตรฐาน	คำอธิบาย	ตัวอย่าง
มาตรฐานความมั่นคงปลอดภัย (Security Specification)	มาตรฐานและเทคโนโลยีต่างๆ ที่สนับสนุนการแลกเปลี่ยนข้อมูลที่มีความมั่นคงปลอดภัย รวมถึงเทคโนโลยีการเข้ารหัสข้อมูล (Encryption) และ Public Key Infrastructure	SSL, TLS, HTTPS, AES, 3DES, Digital Signature
มาตรฐานเปิดอื่นๆ (Others Open Standard Specification)	ครอบคลุมถึงเทคโนโลยีและมาตรฐานเปิดอื่นๆ ที่เป็นที่ยอมรับในระดับสากล	UMM, CCTS, XML NDR, TH e-GIF Version 2.0

กระบวนการตรวจสอบและประเมินคุณภาพข้อมูล (Data Quality)

กระบวนการตรวจสอบและประเมินคุณภาพข้อมูล (Data Quality) สำนักงาน ป.ป.ท. มีความประสงค์ ดำเนินการให้เกิดการตรวจสอบให้ข้อมูลของหน่วยงานมีคุณภาพ ถูกต้อง ครบถ้วน พร้อมใช้อยู่เสมอ โดยยึดตามหลักเกณฑ์การประเมินคุณภาพข้อมูล สำหรับหน่วยงานภาครัฐ (DATA QUALITY ASSESSMENT FRAMEWORK for GOVERNMENT AGENCY) เวอร์ชัน 1.0 โดยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เพื่อเป็นกรอบและเครื่องมือ ในการประเมินคุณภาพข้อมูลของหน่วยงานภาครัฐในการตรวจสอบและควบคุมการบริหารจัดการข้อมูล

มิติคุณภาพข้อมูล	รายละเอียด
ความถูกต้องและสมบูรณ์ (Accuracy and Completeness)	ประเมินเรื่องความถูกต้องแม่นยำ แหล่งข้อมูลที่เชื่อถือได้ และมีกระบวนการตรวจสอบ
ความสอดคล้องกัน (Consistency)	ประเมินเรื่องรูปแบบของข้อมูล ความสอดคล้องกัน และมาตรฐานในการจัดทำข้อมูลของหน่วยงาน
ตรงตามความต้องการของผู้ใช้ (Relevancy)	ประเมินว่าเป็นข้อมูลที่ผู้ใช้ต้องการหรือเป็นข้อมูลที่จำเป็นต้องทราบ มีความละเอียดเพียงพอต่อการนำไปใช้งาน
ความเป็นปัจจุบัน (Timeliness)	ประเมินเรื่องการเผยแพร่ข้อมูล การปรับปรุงข้อมูล และแผนเรื่องระยะเวลา
ความพร้อมใช้ (Availability)	ประเมินความพร้อมใช้ของข้อมูล รวมไปถึงช่องทางในการขอหรือใช้ข้อมูล

สำนักงาน ป.ป.ท. จึงกำหนดมาตรการประเมินคุณภาพ ตามแนวทางข้างต้น ดังนี้

- กำหนดให้มีทีมผู้ประเมินคุณภาพข้อมูล เพื่อทำหน้าที่ การประเมินคุณภาพข้อมูลขององค์กร ประกอบด้วยทีมบริการข้อมูล (Data Stewards Team) ดำเนินการตรวจประเมินคุณภาพข้อมูลอย่างน้อยปีละ 1 ครั้ง ตามรายการในแต่ละมิติตาม DQA Checklist และ DQC Checklist
- กำหนดให้เจ้าของข้อมูล ดำเนินการประเมินตนเองตาม DQA Self-Assessment และนำส่งผลการประเมินให้ทีมผู้ประเมินคุณภาพข้อมูลเพื่อใช้ประกอบการตรวจประเมินคุณภาพข้อมูล
- ในการตรวจประเมินของทีมผู้ประเมินคุณภาพข้อมูล ให้ทีมผู้ประเมินคุณภาพข้อมูลดำเนินการประเมินคุณภาพข้อมูลตามเกณฑ์และวิธีการตรวจประเมินตามที่เจ้าของข้อมูลกำหนด และเจ้าของข้อมูลควรกำหนดเกณฑ์และวิธีการตรวจประเมินให้ชัดเจน และชี้แจงให้ทีมผู้ประเมินคุณภาพข้อมูลรับทราบก่อนทำการประเมิน
- ทีมผู้ประเมินคุณภาพข้อมูล ต้องจัดทำรายงานสรุปผลการตรวจประเมินให้ผู้บริหารรับทราบและดำเนินการตามแผนปฏิบัติการจัดการคุณภาพข้อมูลของหน่วยงานต่อไป

แผนงานการเปิดเผยข้อมูลภาครัฐ

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ ตามที่ราชกิจจานุเบกษา เผยแพร่ ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เมื่อวันที่ 24 มิถุนายน 2563 เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะเพื่อประโยชน์ในการอำนวยความสะดวกแก่ประชาชน ในการเข้าถึงข้อมูล และกำหนดแนวทางและมาตรฐานให้หน่วยงานของรัฐจัดส่งหรือเชื่อมโยงข้อมูลดังกล่าวเปิดเผยแก่ประชาชน ณ ศูนย์กลางข้อมูลเปิดภาครัฐ (Open Government Data of Thailand)

สำนักงาน ป.ป.ท. จึงได้จัดทำแผนงานสำหรับการจัดทำกรเปิดเผยข้อมูลภาครัฐ สำนักงาน ป.ป.ท. ให้สอดคล้องกับแนวทางการตรวจสอบ ปรับปรุงข้อมูล ตามแนวทางธรรมาภิบาลข้อมูลภาครัฐ รวมถึงการพัฒนา ระบบเทคโนโลยีสารสนเทศรองรับการปฏิบัติงาน และการรวบรวม วิเคราะห์ เพื่อให้เกิดความถูกต้องของข้อมูล โดยแผนงานและการขับเคลื่อนเพื่อการเปิดเผยข้อมูลสอดคล้องกับภารกิจของสำนักงาน ป.ป.ท.

แผนงานและกลุ่มกระบวนการ

กระบวนการที่ดำเนินการวิเคราะห์และจัดทำ เพื่อการเปิดเผยข้อมูล	ระยะเวลาดำเนินการ (ไตรมาส - ปีงบประมาณ)												
	๒๕๖๘			๒๕๖๙			๒๕๗๐			๒๕๗๑			
กลุ่มกระบวนการด้านป้องกันการทุจริต													
กระบวนการเครือข่ายประชาสัมพันธ์				x	x	x	x					x	x
กระบวนการส่งเสริมธรรมาภิบาลหน่วยงานรัฐ				x	x	x	x					x	x
กลุ่มกระบวนการด้านปราบปรามการทุจริต													
กระบวนการบริหารจัดการเรื่องร้องเรียน				x	x	x			x	x		x	x
กระบวนการบริหารจัดการคดีการทุจริต				x	x	x			x	x		x	x
กระบวนการด้านกฎหมาย				x	x				x	x		x	x
กลุ่มกระบวนการด้านขับเคลื่อนและกำกับการดำเนินงานนโยบายภาครัฐ													
กระบวนการขับเคลื่อน สปท. และการรายงานข้อร้องเรียนเจ้าหน้าที่รัฐ				x	x	x			x	x		x	x
กระบวนการบริหารความเสี่ยงภาครัฐ				x	x	x			x	x		x	x
กระบวนการบริหารความเสี่ยงโครงการขนาดใหญ่ภาครัฐ				x	x	x	x					x	x
กระบวนการขับเคลื่อนการให้บริการของหน่วยงานภาครัฐ									x	x	x	x	
กลุ่มกระบวนการด้านงานอำนวยการ													
กระบวนการด้านยุทธศาสตร์และแผน				x	x	x	x					x	x
กระบวนการด้านงบประมาณ				x	x	x	x					x	x
กระบวนการด้านการเงิน				x	x	x	x					x	x
กระบวนการด้านบุคลากร				x	x	x	x					x	x
กระบวนการด้านตัวชี้วัดและการประเมิน				x	x	x	x					x	x
กระบวนการด้านคุณธรรมและความโปร่งใส				x	x	x	x					x	x
กระบวนการด้านเทคโนโลยีดิจิทัล			x	x	x	x			x	x		x	x
กระบวนการขับเคลื่อน สปท. สำนักงาน ป.ป.ท.				x	x				x	x		x	x
กระบวนการด้านการตรวจสอบภายใน									x	x	x	x	

คำอธิบายสัญลักษณ์



วิเคราะห์กระบวนการและกำหนดชุดข้อมูล
จัดทำข้อมูล รายละเอียดข้อมูลและเผยแพร่



ทบทวนกระบวนการ ชุดข้อมูลเดิม และชุดข้อมูลใหม่เพิ่มเติม
ทบทวนข้อมูล รายละเอียดข้อมูลและเผยแพร่

กฎหมาย ระเบียบ ประกาศ ที่เกี่ยวข้อง

1. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 และที่แก้ไขเพิ่มเติม
2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม
3. พระราชบัญญัติมาตรการของฝ่ายบริหารในการป้องกันและปราบปรามการทุจริต พ.ศ. 2551 และที่แก้ไขเพิ่มเติม
4. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
5. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
6. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
7. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544
8. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมนูญข้อมูลภาครัฐ พ.ศ. 2563
9. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ พ.ศ. 2563
10. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล ว่าด้วยเรื่อง กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ พ.ศ. 2565
11. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐและแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐ พ.ศ. 2566
12. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล พ.ศ. 2566