แนวปฏิบัติธรรมาภิบาลข้อมูลภาครัฐ และแผนงานการเปิดเผยข้อมูลภาครัฐ

สำนักงานคณะกรรมการป้องกัน
และปราบปรามการทุจริตในภาครัฐ

สารบัญ **หน้า**

นโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูลภาครัฐ
สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

๑. หลักการเหตุผล

สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ (สำนักงาน ป.ป.ท.) เป็นส่วนราชการในฝ่ายบริหารซึ่งรับผิดชอบเกี่ยวกับการป้องกันและปราบปรามการทุจริตในภาครัฐ ตามที่กำหนดในพระราชบัญญัติมาตรการของฝ่ายบริหารในการป้องกันและปราบปรามการทุจริต พ.ศ. ๒๕๕๑ และที่แก้ไขเพิ่มเติม และตามแนวนโยบายของรัฐบาล เป็นศูนย์กลางประสานงานกับหน่วยงานของรัฐที่เกี่ยวข้องทั้งหมด รวมทั้งกำหนดมาตรการต่างๆ เพื่อให้การป้องกันและปราบปรามการทุจริต ดำเนินการบูรณาการงาน ซึ่งในการดำเนินงานตามภารกิจต่างๆ นั้น มีข้อมูลที่ถือเป็นทรัพย์สินสำคัญของสำนักงาน ป.ป.ท. จำเป็นต้องกำหนดสิทธิ หน้าที่ และความรับผิดชอบ ของผู้มีส่วนได้ส่วนเสีย ในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้ได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคลและสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย ตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ประกาศ ณ วันที่ ๑๒ มีนาคม พ.ศ. ๒๕๖๓ กำหนดให้หน่วยงานของรัฐดำเนินการให้เป็นไปตามธรรมาภิบาลข้อมูลภาครัฐ และจัดทำธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงานให้สอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐเพื่อให้การบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วยความสะดวก รวดเร็ว 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)

๒. นิยาม

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

"ข้อมูลเปิด" หมายความว่า ข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้ แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มาหรือตามเจ้าของงานกำหนด

"ชุดข้อมูล" หมายความว่า การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล

"บัญชีข้อมูล" หมายความว่า รายการของชุดข้อมูล ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงานของรัฐ

"เมทาดาตา" หมายความว่า ข้อมูลที่ใช้อธิบายข้อมูล โดยระบุรายละเอียดแหล่งข้อมูล และคำอธิบายรายละเอียดเกี่ยวกับข้อมูล ซึ่งจะทำให้ผู้ใช้ข้อมูลทราบว่าข้อมูลมาจากแหล่งใด มีรูปแบบอย่างไร ช่วยอำนวยความสะดวกในการสืบค้นข้อมูล

"คลังข้อมูล" หมายความว่า ระบบจัดการข้อมูลที่ได้จากการบูรณาการข้อมูลจากหลายแหล่งและในหลายช่วงเวลา มีความสามารถในการเรียก/สืบค้น และรวบรวมข้อมูล ซึ่งข้อมูลที่เก็บรวบรวมบนคลังข้อมูลจะอยู่ในรูปแบบข้อมูลที่มีโครงสร้าง โดยผ่านกระบวนการ Extract Transform Load (ETL) เพื่อให้อยู่ในรูปแบบที่เหมาะสมสำหรับการสร้าง Business Intelligence (BI) และการนำไปวิเคราะห์ข้อมูล

"ดาตาเลค" หมายความว่า แหล่งสำหรับเก็บรวบรวมข้อมูลที่มีหลากหลายรูปแบบ สามารถจัดเก็บข้อมูลที่มีโครงสร้าง ข้อมูลกึ่งโครงสร้าง และข้อมูลที่ไม่มีโครงสร้าง รวมไปถึงข้อมูลดิบที่ไม่มีการเปลี่ยนรูปแบบใดๆ โดยข้อมูลถูกเก็บรักษาไว้ในรูปแบบที่เหมือนหรือใกล้เคียงกับรูปแบบที่ได้รับมาจากแหล่งข้อมูลต้นฉบับ ในการจัดการข้อมูลที่มีปริมาณมาก และหลากหลายรูปแบบ ทำให้เกิดความซับซ้อนในการใช้งานข้อมูลจึงต้องอาศัยผู้เชี่ยวชาญในการจัดการ ได้แก่ Data Engineer เข้ามาช่วยดูแลระบบ, Data Analysis ทำหน้าที่ในการวิเคราะห์ข้อมูล

"ดาตาอนาไลติกส์" หมายความว่า กระบวนการนำข้อมูลมาจัดการโดยการเรียบเรียง จัดระเบียบแยกประเภทชุดข้อมูล ตรวจสอบความถูกต้องของข้อมูล นำมาวิเคราะห์หาความสัมพันธ์ของข้อมูลในรูปแบบต่างๆ จนได้ข้อมูลเชิงลึก เพื่อสรุปหาสาเหตุ ช่วยสนับสนุนการตัดสินใจ หรือกำหนดนโยบายสำคัญขององค์กร

"ธรรมาภิบาลข้อมูลภาครัฐ" คือ การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอนเพื่อให้การได้มาและการนำข้อมูลของหน่วยงานของรัฐไปใช้อย่างถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงแลกเปลี่ยน และบูรณาการระหว่างกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

"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 บุคคลภายนอกและหน่วยงานภายนอกที่ได้รับสิทธิการเข้าถึงข้อมูล

"ความมั่นคงปลอดภัยของข้อมูล" หมายความว่า การดำเนินการตามหลักความมั่นคงปลอดภัยซึ่งประกอบด้วย ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (availability) ของข้อมูล ทั้งนี้เพื่อป้องกันการสูญหายเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลโดยปราศจากอำนาจหรือโดยมิชอบ

๓. ขอบเขต

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

๔. แนวปฏิบัติ

นโยบายและกรอบแนวทางปฏิบัติเพื่อเป็นหลักการในการบริหารจัดการข้อมูลภาครัฐของสำนักงาน ป.ป.ท. มีดังนี้

๔.๑ การเข้าถึงข้อมูล

การบริหารจัดการในการเข้าถึงข้อมูลกำหนดให้ผู้ใช้ข้อมูลต้องนำไปใช้อย่างเหมาะสมและสำนักงาน ป.ป.ท. จะปกป้องข้อมูลด้วยมาตรการรักษาความมั่นคงปลอดภัยที่ได้รับ การรับรองตามมาตรฐานสากล

๔.๒ การนำข้อมูลไปใช้งาน

การสร้างความตระหนักรู้ของผู้ใช้ข้อมูล รวมถึงความรับผิดชอบต่อผลของการนำข้อมูลไปใช้ การเข้าถึงและใช้ข้อมูลตามความจำเป็นในการปฏิบัติงานโดยไม่แสวงหาผลประโยชน์ส่วนตัวหรือเพื่อวัตถุประสงค์อื่นที่ไม่เหมาะสม และใช้ข้อมูลให้เป็นไปตามระดับความปลอดภัยที่กำหนด

๔.๓ การบูรณาการข้อมูลกับหน่วยงานอื่น

สำนักงาน ป.ป.ท. มีการบูรณาการข้อมูลกับหน่วยงานอื่น โดยการจัดส่งข้อมูลเอกสารหรือการเชื่อมโยงข้อมูลผ่านระบบ โดยใช้ข้อมูลเลขประจำตัวประชาชน ๑๓ หลัก หรือ ชื่อ สกุล เป็นเงื่อนไขหลักในการเชื่อมโยง หรือ ตามมาตรฐานการแลกเปลี่ยนข้อมูลระหว่างระบบสารบรรณอิเล็กทรอนิกส์ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือตามมาตรฐานที่มติคณะรัฐมนตรีกำหนด หรือมีการตกลงเป็นลายลักษณ์อักษรเพื่อการเชื่อมโยงข้อมูลระหว่างหน่วยงาน โดยระบบจะทำการประมวลผลและตอบผลข้อมูลรายละเอียดตามแต่ละบริการ

๔.๔ การเก็บรักษาข้อมูล

สำนักงาน ป.ป.ท. ไม่มีหน้าที่ในการจัดเก็บข้อมูลของหน่วยงานที่แลกเปลี่ยนเชื่อมโยงข้อมูล แต่จะทำการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลการใช้งานของผู้ใช้ข้อมูลที่สอดคล้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม

๔.๕ การเปิดเผยข้อมูล

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

๔.๖ การเผยแพร่และการทบทวน

สำนักงาน ป.ป.ท. อาจจะพิจารณาทบทวนหรือแก้ไขปรับปรุงแนวปฏิบัติฉบับนี้เพื่อให้สอดคล้องกับกฎหมาย ระเบียบ หรือนโยบายที่เกี่ยวข้อง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

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

หมวดหมู่และการจัดระดับชั้นของข้อมูล ซึ่งข้อมูลของหน่วยงานสามารถแบ่งหมวดหมู่ตามกรอบธรรมาภิบาลข้อมูลและการใช้งานของสำนักงาน ป.ป.ท. ได้ดังนี้

ข้อมูลที่มีชั้นความลับ (Secret) แบ่งเป็น ข้อมูลลับที่สุด (Top Secret) ข้อมูลลับมาก (Secret) และข้อมูลลับ (Confidential)

ข้อมูลภายในองค์กร (Internal Use) ได้แก่ ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงานซึ่งไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาต

ข้อมูลสาธารณะ และข้อมูลเปิดเผยได้ (Public) ได้แก่ ข้อมูลที่สามารถเปิดเผยบุคคลทั่วไป โดยไม่ก่อให้เกิดความเสียหาย

การเผยแพร่และการทบทวน

แนวปฏิบัติการดำเนินงานด้านธรรมาภิบาลข้อมูลนี้จะต้องทำการเผยแพร่โดยการประกาศในเว็บไซต์สำนักงาน ป.ป.ท. เพื่อให้เจ้าหน้าที่รับทราบ และถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด ซึ่งแนวปฏิบัตินี้จะต้องถูกทบทวนอย่างน้อยปีละ ๑ ครั้ง รวมถึงเมื่อมีข้อเสนอแนะจากคณะกรรมการข้อมูลข่าวสารและเปิดเผยข้อมูลภาครัฐ ของสำนักงาน ป.ป.ท.

หมวด ๑ การสร้างข้อมูล

กระบวนการสร้างข้อมูล เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติ ด้วยอุปกรณ์อิเล็กทรอนิกส์ รวมถึงการซื้อข้อมูล หรือการรับข้อมูลมาจากหน่วยงานอื่นเพื่อนำมาจัดเก็บในภายหลัง

กิจกรรม	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล	x		
กำหนดชั้นความลับข้อมูลของข้อมูลที่ถูกสร้างขึ้น	x		
กำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูล			x
จัดทำคำอธิบายชุดข้อมูลดิจิทัล	x	x	
ประเมินคุณค่าของชุดข้อมูลดิจิทัล	x	x	
ตรวจสอบความถูกต้องของข้อมูล	x		

๑. เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิ์ในการสร้างข้อมูล และจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับ โครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

๒. เจ้าของข้อมูลเป็นผู้กำหนดชั้นความลับของข้อมูลที่ถูกสร้างขึ้นตามวิธีปฏิบัติการจำแนกชั้นความลับของข้อมูล

๓. เจ้าของข้อมูลกำหนดให้มีวิธีปฏิบัติการจำแนกชั้นความลับข้อมูลสำหรับข้อมูลที่ถูกสร้างขึ้น

๔. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการสร้างข้อมูลให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด

๕. เจ้าของข้อมูลร่วมกับบริกรข้อมูล ร่วมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา

(Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานคำอธิบายชุดข้อมูลดิจิทัลที่ สำนักงาน ป.ป.ท. กำหนด และสอดคล้องกับมาตรฐานที่ภาครัฐได้กำหนดไว้

๖. เจ้าของข้อมูลร่วมกับบริกรข้อมูลทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมิน คุณค่าชุดข้อมูลที่ สพร. หรือสำนักงาน ป.ป.ท. กำหนดและเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล

๗. ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่มีลักษณะดังต่อไปนี้ เข้าสู่ระบบคอมพิวเตอร์ที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

- ข้อมูลที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลอันเป็นเท็จ ซึ่งจะเกิดความเสียหายแก่ประชาชน
- ข้อมูลอันเป็นเท็จที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือโครงสร้างพื้นฐาน หรือก่อให้เกิดความตื่นตระหนก
- ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือความผิดเกี่ยวกับการก่อการร้าย
- ข้อมูลที่มีลักษณะอันลามก และประชาชนทั่วไปอาจเข้าถึงได้
- ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดทำให้ผู้อื่นเสียชื่อเสียง

๘. ห้ามมิให้ผู้สร้างข้อมูลทำการสร้าง ทำซ้ำหรือดัดแปลงต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่นเว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง

๙. กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น

๑๐. กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น

๑๑. กำหนดให้มีวิธีปฏิบัติเกี่ยวกับสร้างข้อมูลให้มีความปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล

หมวด ๒ การจัดเก็บข้อมูล

กระบวนการจัดเก็บข้อมูล เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือข้อมูลที่ได้จากการ แลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลาย และให้ผู้ใช้งานสามารถ ประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว

กิจกรรม	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดระยะเวลาในการจัดเก็บข้อมูล	x		
ตรวจสอบความครบถ้วนของชุดข้อมูลหรือเมทาดาตา ของการจัดเก็บชุดข้อมูล	x	x	
ทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดเพื่อจัดเก็บเป็นข้อมูลถาวร		x	x
จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์			x

๑. เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน

๒. กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลหรือเมทาดาตา หากไม่มีหรือไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูลและบริกรข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน

๓. บริกรข้อมูลและผู้ดูแลระบบสารสนเทศ ทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้ว เพื่อจัดเก็บเป็นข้อมูลถาวร

๔. การจัดเก็บข้อมูลที่มีชั้นความลับให้ทำการเข้ารหัสข้อมูล เพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

๕. กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ เพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่า ด้วยการกระทำความผิดทางคอมพิวเตอร์

๖. กำหนดให้การจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้

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

- มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบสามารถแก้ไขข้อมูล ที่เก็บรักษาไว้

- การจัดเก็บข้อมูลต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้ (Identification and Authentication)

๗. กรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บดังนี้

- เก็บในสถานที่ที่มีมาตรการป้องกันการเข้าถึงข้อมูล เช่น สามารถปิดล็อคได้เมื่อไม่ใช้งาน

- เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ ได้แก่ เครื่องถ่ายเอกสาร เครื่องพิมพ์ เป็นต้น เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์ในการเข้าถึงข้อมูลได้

๘. กำหนดให้มีการจัดเก็บข้อมูลส่วนบุคคล โดยให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๙. กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่ จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความ เสียหายต่อหน่วยงาน

๑๐. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่อง ทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

๑๑. ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของสำนักงาน สำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่สำนักงานจัดสรรไว้

หมวด ๓ การใช้ข้อมูล

กระบวนการใช้ข้อมูล (Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยน รูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน รวมถึงการสำรอง (Backup) ข้อมูล เพื่อเป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึก ข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

กิจกรรม	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดสิทธิ์ประมวลผลและเข้าใช้งานข้อมูลตามชั้นความลับ	x		
กำหนดสิทธิ์ในการประมวลผลและเข้าใช้งานข้อมูลให้แก่ผู้ใช้ข้อมูล			x
ทบทวนสิทธิ์การเข้าถึงและการใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง	x		

๑. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้

- ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิ์ตามตำแหน่ง/บทบาท เท่านั้น
- ข้อมูลใช้ภายใน กำหนดให้ผู้บริหาร ข้าราชการ ลูกจ้าง และเจ้าหน้าที่ของรัฐเท่านั้น ที่มีสิทธิ์เข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้ ทั้งนี้ ต้องปกป้องข้อมูลจากการเข้าถึงโดยบุคคลภายนอก
- ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล

๒. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการเข้าถึงเพื่อประมวลผล และใช้ข้อมูลผู้ใช้งานตามที่ เจ้าของข้อมูลกำหนด

๓. เจ้าของข้อมูลจะต้องทบทวนสิทธิ์การเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ได้แก่ การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ

๔. ผู้ที่มีสิทธิ์เข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูลจะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ

๕. ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของหน่วยงาน เพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือเพื่อ เข้าสู่เว็บไซต์ที่ไม่เหมาะสม หรือใช้ข้อมูลอันก่อนให้เกิดความเสียหายต่อหน่วยงาน

หมวด ๔ การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

เพื่อกำหนดแนวปฏิบัติและมาตรฐานด้านเทคนิคในการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลทั้งภายใน หน่วยงานและระหว่างหน่วยงานอย่างมีประสิทธิภาพ และก่อให้เกิดประโยชน์ต่อภาครัฐ ภาคเอกชน และประชาชน โดยเป็นการเชื่อมโยงและแลกเปลี่ยนข้อมูล ให้มีความมั่นคงปลอดภัย น่าเชื่อถือ และข้อมูลมีคุณภาพ สามารถนำไปใช้ ประโยชน์ได้อย่างมีประสิทธิภาพ

กิจกรรม	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดแนวทาง/กระบวนการ ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล	x	x	
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาและตรวจสอบชั้นความลับของข้อมูล	x	x	x
กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล			x
กำหนดมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล		x	x
จัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการ			x

แลกเปลี่ยนข้อมูลดิจิทัลที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File)			
ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำไปใช้		x	x

๑. กำหนดให้เจ้าของข้อมูลหรือบริกรข้อมูล จัดทำแนวทาง/กระบวนการ ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล โดยมีองค์ประกอบ ดังต่อไปนี้เป็นอย่างน้อย

๒. กำหนดให้เจ้าของข้อมูล หรือบริกรข้อมูลตามที่ได้รับมอบหมายดำเนินการตรวจสอบคำอธิบายชุดข้อมูล ดิจิทัลหรือเมทาดาตาของข้อมูลที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน

๓. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

๔. บริกรข้อมูลร่วมกับร่วมกับผู้ดูแลระบบสารสนเทศ กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัย เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์หรือส่ง ข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้ รับอนุญาต

๕. กำหนดให้ผู้ดูระบบสารสนเทศต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยง และการแลกเปลี่ยนข้อมูลดิจิทัล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

๖. บริกรข้อมูลร่วมกับร่วมกับผู้ดูแลระบบสารสนเทศ ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยน ข้อมูลและการนำไปใช้

๗. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูล ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการ กระทำความผิดทางคอมพิวเตอร์

หมวด ๕ การเผยแพร่และการเปิดเผยข้อมูล

เพื่อกำหนดแนวปฏิบัติและมาตรฐานการเผยแพร่และการเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอด ในการพัฒนาในรูปแบบต่าง ๆ ได้ โดยการเปิดเผยข้อมูลเป็นการนำข้อมูลที่อยู่ในครอบครองของหน่วยงานเผยแพร่ตาม ช่องทางต่าง ๆ อย่างเหมาะสม ทั้งการเปิดเผยตามนโยบายรัฐและการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

กิจกรรม	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ง่าย	x	x	
คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด (Open Data)	x	x	
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาของชุดข้อมูลที่จะทำการเปิดเผยให้มีความครบถ้วนเป็นปัจจุบัน	x	x	
กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย	x	x	

๑. เจ้าของข้อมูลร่วมกับบริกรข้อมูล กำหนดช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ง่าย

๒. กำหนดให้เจ้าของข้อมูลร่วมกับบริกรข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด

จากลำดับชั้น ความสำคัญของชุดข้อมูล

๓. เจ้าของข้อมูลร่วมกับบริกรข้อมูล คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิด (Open Data) ใน รูปแบบข้อมูลเปิดของสำนักงาน ป.ป.ท.

๔. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และต้องเปิดเผยข้อมูลในรูปแบบ ดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (data.go.th) และระบบบัญชีภาครัฐ (gdcatalog.go.th)

๕. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

๖. เจ้าของข้อมูลข้อมูลห้ามเปิดเผยข้อมูลความมั่นคง และข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงาน ยกเว้นได้รับการอนุมัติจากสำนักงาน ป.ป.ท. รวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบาย และแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงานเจ้าของข้อมูล

หมวด ๖ การทำลายข้อมูล

เพื่อกำหนดแนวปฏิบัติการทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ เพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล

กิจกรรม	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้ทำลาย
กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล	x	x		
กำหนดสิทธิ์ในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูล			x	
ทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน				x
จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง	x	x		
จัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี				x
ทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอหรือข้อมูลส่วนบุคคลที่พ้นระยะเวลาการเก็บรักษาตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล				x

๑. เจ้าของข้อมูลร่วมกับบริการข้อมูล กำหนดผู้มีสิทธิ์ในการทำลายข้อมูล หรือทำให้ข้อมูลส่วนบุคคลเป็น ข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคลได้ และจะต้องทบทวนสิทธิ์นั้นอย่างน้อยปี ละ ๑ ครั้ง

๒. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการทำลายข้อมูลให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด

๓. ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ป.ป.ท.

๔. กำหนดให้เจ้าของข้อมูลร่วมกับบริกรข้อมูล จัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลาย สำหรับตรวจสอบในภายหลัง

๕. กำหนดให้ผู้ทำลายข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยเก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี

๖. กำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ โดยจะต้องผ่านการเห็นชอบจากผู้ควบคุมข้อมูลส่วนบุคคล และดำเนินการตามข้อกำหนดที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนดไว้อย่างเคร่งครัด

๕. กระบวนการ

ขั้นตอนที่ใช้สำหรับกำกับ ดูแลการดำเนินการใด ๆ ต่อข้อมูลให้เป็นไปตามกฎหมาย ระเบียบ หรือนโยบายที่เกี่ยวข้องกับข้อมูลมีรายละเอียดและแนวปฏิบัติ ดังต่อไปนี้

๕.๑ การสร้างข้อมูล

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

๕.๑.๒ จัดชั้นความลับของข้อมูลที่จะเก็บรวบรวม ใช้ หรือเปิดเผย

๕.๑.๓ จัดให้มีคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐและบัญชีข้อมูลจากข้อมูลต่าง ๆ ที่รวบรวมให้มีความถูกต้อง ครบถ้วนและเป็นปัจจุบัน

๕.๒ การจัดเก็บข้อมูลและการทำลายข้อมูล

๕.๒.๑ การเก็บข้อมูล สำนักงาน ป.ป.ท. จะใช้วิธีตามที่กฎหมายกำหนดในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล โดยสำนักงาน ป.ป.ท. จะเก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัดและเท่าที่จำเป็น ตามวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล

๕.๒.๒ การจัดเก็บ การจัดเก็บถาวร ต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและความเป็นส่วนบุคคลของข้อมูล ให้เป็นไปตามที่กฎหมายกำหนด หรือแนวปฏิบัติในการปกป้องข้อมูลหรือแนวปฏิบัติในด้านความมั่นคงปลอดภัยและชั้นความลับของข้อมูล

๕.๒.๓ การจัดเก็บข้อมูล ต้องจัดเก็บลงในสื่อบันทึกข้อมูลและมีโครงสร้างข้อมูลตามมาตรฐานสถาปัตยกรรมข้อมูล ข้อมูลหลัก และข้อมูลอ้างอิง

๕.๒.๔ การจัดเก็บถาวร ต้องเป็นการดำเนินการกับข้อมูลที่ไม่มีการลบ ปรับปรุง หรือแก้ไขอีกต่อไปและสามารถนำกลับมาใช้งานได้ โดยให้เป็นไปตามที่กฎหมายกำหนด

๕.๒.๕ การจัดเก็บข้อมูลชั้นความลับที่เป็นข้อมูลความลับทางราชการ และข้อมูลความมั่นคงต้องมีการเข้ารหัสข้อมูล

๕.๒.๖ การสำรองข้อมูล ต้องจัดเก็บให้มีความถูกต้องครบถ้วนเป็นปัจจุบัน ตามมาตรฐานการสำรองข้อมูล

๕.๒.๗ การทำลายข้อมูล ต้องเป็นการดำเนินการกับข้อมูลที่ไม่ต้องนำกลับมาใช้งานได้อีกต่อไปโดยให้เป็นไปตามที่กฎหมายกำหนด

๕.๓ การประมวลผลข้อมูลและการใช้ข้อมูล

๕.๓.๑ สิทธิการประมวลผลข้อมูลและการใช้งานของผู้ใช้ข้อมูล ให้เป็นตามวัตถุประสงค์ของการใช้งานและคำนึงถึงขั้นความลับของข้อมูล โดยให้เป็นไปตามที่กฎหมายกำหนด

๕.๓.๒ การประมวลผลข้อมูลและการใช้ข้อมูลต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ตามแนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคล และแนวปฏิบัติในด้านความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล โดยให้เป็นไปตามที่กฎหมายกำหนด

๕.๓.๓ การประมวลผลและการใช้ข้อมูล ต้องมีความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องการ (Consistency) ความเป็นปัจจุบัน (Timeliness) และมีคุณภาพ (Quality)

๕.๓.๔ การเรียกใช้ข้อมูลชั้นความลับที่เป็นข้อมูลความลับทางราชการ และข้อมูลความมั่นคงต้องมีการกำหนดสิทธิการเข้าใช้ข้อมูล

๕.๓.๕ ต้องจัดให้มีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล เพื่อให้สามารถตรวจสอบย้อนกลับได้ โดยให้เป็นไปตามที่กฎหมายกำหนด

๕.๓.๖ ผู้ใช้ข้อมูลจะต้องเป็นผู้รับผิดชอบ หากมีการประมวลผลข้อมูลและการใช้ข้อมูลที่ไม่เป็นไปตามที่กฎหมายกำหนด

๕.๔ การเปิดเผยข้อมูล

๕.๔.๑ การเปิดเผยข้อมูลต่าง ๆ จะต้องเป็นไปตามที่กฎหมายกำหนด

๕.๔.๒ สำนักงาน ป.ป.ท. จะเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลในกรณีใดกรณีหนึ่งดังต่อไปนี้

๑) ได้รับความยินยอมจากเจ้าของข้อมูล

๒) เป็นความจำเป็นเพื่อการปฏิบัติงานของราชการหรือตามคำขอของเจ้าของข้อมูล รวมทั้งเปิดเผยเพื่อให้การทำธุรกรรมหรือกิจกรรมใด ๆ ของเจ้าของข้อมูลสามารถดำเนินการได้โดยบรรลุตามวัตถุประสงค์ของเจ้าของข้อมูล

๓) เป็นความจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมาย

๔) เป็นการปฏิบัติงานตามกฎหมายหรือกฎเกณฑ์ของทางราชการหรือคำสั่งของหน่วยงานที่มีอำนาจกำกับดูแล หรือที่มีอำนาจตามกฎหมาย

๕.๔.๓ การเผยแพร่ข้อมูลหรือการเปิดเผยข้อมูลในรูปแบบดิจิทัล ต้องปฏิบัติตามแนวทางการเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบดิจิทัลต่อสาธารณะของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

๕.๕ การเชื่อมโยงและการแลกเปลี่ยนข้อมูล

๕.๕.๑ การเชื่อมโยงและการแลกเปลี่ยนข้อมูลของสำนักงาน ป.ป.ท. กับหน่วยงานอื่น ๆ จะต้องได้รับอนุญาตจากสำนักงาน ป.ป.ท. และมีความร่วมมือ หรือแนวทางในด้านการบริหารจัดการข้อมูลกับหน่วยงานนั้น ๆ อย่างชัดเจน

๕.๕.๒ การเชื่อมโยงและการแลกเปลี่ยนข้อมูล ต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ตามแนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคล และแนวปฏิบัติในด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยให้เป็นไปตามที่กฎหมายกำหนด

๕.๕.๓ เทคโนโลยีและวิธีการทางเทคนิคที่เกี่ยวข้องกับการเชื่อมโยงและการแลกเปลี่ยนข้อมูลให้เป็นไปตามมาตรฐานสากล

๕.๖ การติดตามและประเมินผลการใช้งานข้อมูลสำนักงาน ป.ป.ท. จะกำหนดให้มีการติดตามและประเมินผลการใช้งานข้อมูลอย่างน้อยปีละ ๑ ครั้ง โดยจัดทำเป็นรายงานเสนอไปยังผู้บริหาร

๖. โครงสร้างของบุคลากรที่รับผิดชอบ

๖.๑ หัวหน้าหน่วยงาน (Chief Executive Officer : CEO)

ผู้รับผิดชอบ เลขาธิการคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

มีหน้าที่ ตัดสินใจเชิงนโยบายแก้ไขปัญหา บริหารจัดการและสนับสนุนธรรมาภิบาลข้อมูลภายในหน่วยงาน

๖.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer : DCIO)

ผู้รับผิดชอบ ผู้บริหารระดับสูงที่ได้รับมอบหมายให้กำกับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

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

๖.๓ คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee)

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

มีหน้าที่ ให้คำปรึกษา กำกับดูแลข้อมูล พร้อมเสนอแนะนโยบายและแนวทางการบริหารจัดการข้อมูล

๖.๔ ผู้บริหารข้อมูลระดับสูง (Chief Data Officer : CDO)

ผู้รับผิดชอบ ผู้บริหารที่ได้รับมอบหมาย

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

๖.๕ เจ้าของข้อมูล (Data Owner)

ผู้รับผิดชอบ หัวหน้าหน่วยงานผู้มีหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง

มีหน้าที่ รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือ กฎหมาย เจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่ง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การเปลี่ยนแปลง Metadata และเกณฑ์การทำ Data Cleansing รวมถึงการกำหนดสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

๖.๖ ทีมบริกรข้อมูล (Data Stewards Team)

ผู้รับผิดชอบ ประกอบด้วย หัวหน้าบริกรข้อมูล (Lead Data steward) บริกรข้อมูลด้านธุรกิจ บริการข้อมูลด้านเทคนิค บริกรข้อมูลด้านคุณภาพข้อมูล รวมไปถึงบุคคลที่ทำหน้าที่เกี่ยวกับความมั่นคงปลอดภัย กฎหมาย และบุคคลที่ให้ความรู้เกี่ยวกับนโยบายข้อมูลและความรู้อื่น ๆ

มีหน้าที่ ต้องดำเนินการดังนี้

๑) กำหนด ทบทวนความต้องการด้านคุณภาพข้อมูล การรักษาความเป็นส่วนบุคคล และความมั่นคงปลอดภัยของข้อมูล

๒) กำหนด ทบทวน และปรับปรุงกระบวนการให้สอดคล้องกับนโยบายข้อมูล เป้าประสงค์ ความต้องการของผู้มีส่วนได้เสียกับข้อมูล รวมทั้งติดตามการดำเนินงานตามแผนที่กำหนดเพื่อนำมาปรับปรุงกระบวนการทำงาน

๓) กำหนดนิยามคำอธิบายชุดข้อมูลดิจิทัล พร้อมทั้งจัดทำบัญชีข้อมูลให้ครบถ้วนตามความจำเป็นในการใช้งาน และตรงตามความต้องการของผู้มีส่วนได้เสียกับข้อมูล

๔) วิเคราะห์ความพร้อมของธรรมาภิบาลข้อมูล ความต้องการด้านคุณภาพข้อมูล การรักษาความเป็นส่วนบุคคล และความมั่นคงปลอดภัยให้เหมาะสมกับสถานการณ์ปัจจุบัน เพื่อวางแผนการวัดและประเมินผล

๕) ตรวจสอบ วิเคราะห์ วัดผลการดำเนินงาน

๖) ให้ข้อเสนอแนะเชิงเทคนิคที่สอดคล้องกับนโยบาย เป้าประสงค์ และความต้องการของผู้มีส่วนได้เสียกับข้อมูล

๗) กำหนดรายละเอียดที่เกี่ยวข้องกับการออกแบบระบบเทคโนโลยีสารสนเทศ รวมถึงโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ เพื่อคุ้มครองข้อมูลส่วนบุคคล และรักษาความมั่นคงปลอดภัย

๘) สนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศและอื่น ๆ ที่เกี่ยวข้อง

๙) รายงานผลลัพธ์ไปยังคณะกรรมการดิจิทัล สำนักงาน ป.ป.ท. และผู้เกี่ยวข้อง

๖.๗ ทีมบริหารจัดการข้อมูล (Data Management Team)

ผู้รับผิดชอบ ประกอบด้วย เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และเจ้าหน้าที่ที่ได้รับมอบหมายของหน่วยงาน

มีหน้าที่ ต้องดำเนินการบริหารจัดการข้อมูล ตามองค์ประกอบดังนี้

๑) สถาปัตยกรรมข้อมูล (Data Architecture)

๒) การจำลองและการออกแบบข้อมูล (Data Modeling and Design)

๓) การจัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operation)

๔) การบูรณาการและความสามารถในการทำงานร่วมกัน (Data Integration and Interoperability)

๕) การบริหารจัดการเอกสารและเนื้อหา (Document and Content Management)

๖) ข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data)

๗) คลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะ และดาตาอนาไลติกส์

๘) คำอธิบายชุดข้อมูลดิจิทัล หรือ Metadata

๙) ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy)

๑๐) คุณภาพของข้อมูล (Data Quality)

๖.๘ ผู้สร้างข้อมูล (Data Creators)

ผู้รับผิดชอบ เจ้าหน้าที่ของหน่วยงานที่เป็นเจ้าของข้อมูล

มีหน้าที่ บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ รวมถึงทำงานร่วมกับทีมบริกรข้อมูล เพื่อตรวจสอบ แก้ไขด้านคุณภาพ และความมั่นคงปลอดภัยข้อมูล

๖.๙ ผู้ใช้ข้อมูล (Data Users)

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

มีหน้าที่ นำข้อมูลไปใช้งาน ต้องสนับสนุนธรรมาภิบาลข้อมูลภาครัฐ โดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังทีมบริกรข้อมูล

การควบคุมสิทธิ์การเข้าถึงข้อมูล (Access Control)

สำนักงาน ป.ป.ท. ได้กำหนดแนวทางการควบคุมสิทธิ์การเข้าถึงข้อมูลของหน่วยงาน เพื่อให้การบริหารจัดการข้อมูลเป็นไปอย่างมีประสิทธิภาพ โดยมีรายละเอียด ดังนี้

๑. การเข้าถึงข้อมูลผ่านระบบสารสนเทศ

๑) ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ ต่อเมื่อได้รับอนุญาตจาก ผู้รับผิดชอบ/เจ้าของข้อมูล/ ตามความจำเป็นต่อการใช้งาน เท่านั้น

๒) บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้อง ขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารระดับสูง หรือหัวหน้าหน่วยงานแล้วแต่กรณี เพื่อให้ความเห็นชอบ และอนุญาตก่อน

๓) ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งาน และหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศ รวมทั้งมีการทบทวน สิทธิ์การเข้าถึงอย่างสม่ำเสมอ โดยผู้ดูแลระบบจะเป็นผู้กำหนดสิทธิ์ตามอนุญาตนั้น ดังนี้

๓.๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจ ดังนี้

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

๓.๒) กำหนดเกณฑ์การระงับสิทธิ์มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

๓.๓) ผู้ดูแลระบบมีหน้าที่ควบคุมดูแลการเข้าถึงระบบสารสนเทศและปฏิบัติงานตามหัวหน้าหน่วยงานมอบหมาย ดังนี้

- อนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของหน่วยงานจะกระทำได้ต่อเมื่อได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย
- กำหนดสิทธิ์ของผู้ใช้งานให้เหมาะสมกับการใช้งานและทบทวนสิทธิ์ การเข้าถึงนั้นอย่างสม่ำเสมอ
- ติดตั้งระบบการบันทึกและติดตามการใช้งานและตรวจตราการละเมิด ความปลอดภัยที่มีต่อระบบสารสนเทศของหน่วยงานอย่างสม่ำเสมอ

๔) จัดแบ่งประเภทของข้อมูล ชั้นความลับ ตามมาตรฐาน นโยบายแนวปฏิบัติที่สำนักงาน ป.ป.ท. กำหนด รวมถึงระดับชั้นการเข้าถึง เวลาเข้าถึง และช่องทางการเข้าถึงข้อมูลไว้ให้ชัดเจนโดยใช้แนวทางตามระเบียบที่เกี่ยวข้อง โดยจัดแบ่งระดับชั้นการเข้าถึง อย่างน้อย ดังนี้

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๕) เจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูล ของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ ยังคงมีความเหมาะสม

๖) ระบบงานสารสนเทศที่มีการเชื่อมโยงข้อมูลกันให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและ

การสื่อสารพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัยๆ ก่อนตัดสินใจ ใช้ข้อมูลร่วมกันในระบบงานหรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน โดยมีประเด็นต้องดำเนินการอย่างน้อย ดังนี้

๖.๑) กำหนดนโยบายและมาตรการเพื่อควบคุมดูแล และบริหารจัดการการใช้ข้อมูลร่วมกัน

๖.๒) พิจารณาจำกัดหรือการอนุญาตการเข้าถึงข้อมูลส่วนบุคคล

๖.๓) พิจารณาว่ามีบุคคล กลุ่มบุคคล ที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

๖.๔) พิจารณาเกี่ยวกับระบบการลงทะเบียนและบริหารสิทธิ์ผู้ใช้งาน

๖.๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

แนวปฏิบัติสำหรับแบ่งปันและแลกเปลี่ยนข้อมูล (Shareable Data)

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

ผู้รับผิดชอบ

๑. เจ้าของข้อมูล (Data Owners)

๒. คณะบริกรข้อมูล (Data Stewards)

๓. ผู้ดูแลระบบ (Data Owners)

๔. ผู้จัดการโครงการ (Project Managers)

๕. ทีมบริหารจัดการข้อมูล (Data Management Team)

กระบวนการขั้นตอนการปฏิบัติงาน

๑. กำหนดให้ผู้จัดการโครงการกำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการในความรับผิดชอบ ดังนี้

๑.๑ การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน กำหนดให้ใช้รูปแบบที่เป็นมาตรฐานเปิด (Open Format) ทั้งในส่วนมาตรฐานข้อมูล เช่น XML และ JSON เป็นต้น มาตรฐานโปรโตคอลสื่อสาร เช่น SOAP REST หรืออื่น ๆ ที่ได้รับการยอมรับจากมาตรฐานสากล

๑.๒ การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ให้ดำเนินการตามมาตรฐานกลางของหน่วยงานหลักที่เป็นผู้รับผิดชอบ

๒. กำหนดให้ผู้จัดการโครงการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่จะ ทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้

๒.๑ ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้

๒.๒ ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ นั่นคือ ต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็น ส่วนตัว พร้อมทั้งตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจตามกฎหมาย ของหน่วยงานนั้น ๆ

๒.๓ หากไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริกรข้อมูลธุรกิจ บริกรข้อมูลเทคนิคและทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

๓. ในกรณีที่มีหน่วยงานอื่นที่ไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูล ส่วนบุคคล ในการครอบครองของหน่วยงาน เพื่อทำการศึกษาหรือวิจัย ซึ่งเป็นข้อยกเว้นตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ให้หน่วยงานเจ้าของข้อมูลอนุญาตหน่วยงานนั้นในการเชื่อมโยงข้อมูลได้ โดยจะต้องแสดงข้อมูลนั้นด้วยวิธีไม่แสดงตัวตน (Anonymization)

๔. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลเพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต

๕. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

๖. กำหนดให้ผู้ดูระบบแม่ข่ายต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลเพื่อใช้ตรวจสอบสิ่งผิดปกติต่างๆ ที่เกิดขึ้นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

กิจกรรม	ผู้จัดการโครงการ	ผู้ดูแลระบบแม่ข่าย	เจ้าของข้อมูล	บริกรข้อมูล
กำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นในการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการ	R	S	I	I
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัล และชั้น ความลับของข้อมูล	R	R	C	C
จัดทำแนวทางการทำงานร่วมกันทั้งระหว่าง หน่วยงานภายในและหน่วยงานภายนอกใน การเชื่อมโยงและแลกเปลี่ยนข้อมูล	R	S	S	S
จัดเก็บบันทึกหลักฐานของการเชื่อมโยง และ การแลกเปลี่ยนข้อมูลดิจิทัล	I	R	I	I

R (Response): รับผิดชอบในการทำงานหรือปฏิบัติงาน, S (Support): สนับสนุน,
I (Inform): ได้รับข้อมูลเกี่ยวกับความคืบหน้า, C (Consult): เสนอแนะและให้ความเห็น

มาตรฐานการเชื่อมโยงและการแลกเปลี่ยนข้อมูล

สำนักงาน ป.ป.ท. มีแนวทางการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัลทั้งภายในหน่วยงานและระหว่างหน่วยงาน รายละเอียดดังตารางต่อไปนี้

หมวดมาตรฐาน	คำอธิบาย	ตัวอย่าง
มาตรฐานการเชื่อมโยง (Interconnection Specification)	รายการมาตรฐานที่ใช้ในการเชื่อมโยงระบบข้อมูล รวมถึงระบุ แนวทางการเชื่อมโยงในระดับ โปรโตคอลมาตรฐาน ต่างๆ	HTTP: Hypertext Transfer Protocols SMTP: E-mail Transport POP๓, IMAP: Mailbox Access FTP: Fire Transfer SMS: Short Message Service
มาตรฐานการแลกเปลี่ยนข้อมูล (Data Exchange Specification)	รายการมาตรฐานเพื่อการแลกเปลี่ยนข้อมูล ครอบคลุมถึง เทคโนโลยีและมาตรฐานต่างๆ สำหรับการจัดโครงสร้างข้อมูล (Structure) และการเข้ารหัสข้อมูล (Encode) เพื่อการแลกเปลี่ยนข้อมูล	XML: Extensible Markup Language
มาตรฐานรูปแบบการ	มาตรฐานและเทคโนโลยีที่เกี่ยวข้องกับการนำเสนอ	XML Schema:

จัดเก็บและนำเสนอข้อมูล (Storage &Presentation Specification)	สารสนเทศ มาตรฐานเหล่านี้ช่วยให้สารสนเทศสามารถถูกนำมาแสดงผลได้ในรูปแบบที่สอดคล้องกันโดยเฉพาะอย่างยิ่งเมื่อต้องมีการแบ่งปันข้อมูลระหว่างต่างระบบกัน ทั้งมาตรฐาน รูปแบบของสื่อที่เป็น image และ streaming media ต่างๆ และมาตรฐานเอกสารอิเล็กทรอนิกส์	Extensible Markup Language Schema RSS: RDF Site Summary XLS, XLSX: Microsoft Excel Spread Sheet CSV: Comma-separated Value E-R Diagram: Entity Relation Diagram
บริการผ่านเว็บเซอร์วิสเทคโนโลยี (Web Technology Specification)	มาตรฐานและเทคโนโลยีที่เกี่ยวเว็บ เซอร์วิสเพื่อการแลกเปลี่ยนข้อมูล ระหว่าง ระบบที่มีแพลต์ฟอร์ม เหมือนกันและแตกต่างกัน	SOAP: Simple Object Access Protocol UDDI: Universal Description Discovery and Integration WSDL: Web Services Description Language
บริการด้านธุรกรรม (Business Service Specification)	มาตรฐานและเทคโนโลยีในกลุ่มงานธุรกรรมที่มีเทคนิคเฉพาะด้านของกลุ่มงานนั้น	ebXMLbusiness repositories Registry Information Model (ebRIM) RIM v๓.๐ Registry Service Specification (ebRS) RS v๓.๐ ebXMLMessage Service Message Service Specifiction(ebMS) ebMSV๒.๐

มาตรฐานความมั่นคงปลอดภัย (Security Specification)	มาตรฐานและเทคโนโลยีต่างๆ ที่ สนับสนุนการแลกเปลี่ยนข้อมูลที่มี ความมั่นคงปลอดภัย รวมถึงเทคโนโลยีและมาตรฐานต่างๆ สำหรับการเข้ารหัสข้อมูล (Encryption) และ Public key infrastructure ที่ใช้เป็นมาตรฐาน สนับสนุนการใช้กุญแจสาธารณะ (public key) และกุญแจส่วนบุคคล (private key) เพื่อการเข้ารหัส (Encryption) และถอดรหัส (Decryption) มาตรฐาน Digital Signature และ โปรโตคอลการส่งข้อมูลที่มีความมั่นคงปลอดภัยสูง	Secure mailbox access SSL: Secure Socket Layer TLS: Transport Layer Security Transport security SSL: Secure Socket Layer TLS: Transport Layer Security HTTPS: Hyper Text Transfer Protocol over Secure Socket Layer Encryption algorithms AES: Advanced Encryption Standard ๓DES: Triple Data Encryption Standard
มาตรฐานเปิดอื่นๆ (Others Open Standard Specification)	ครอบคลุมถึงเทคโนโลยีและมาตรฐานเปิดอื่นๆ ที่เป็นที่นิยมในระดับสากล	ขั้นตอนการพัฒนาระบบงาน UMM: UN/CEFACT Modeling Methodology การจัดทำมาตรฐานข้อมูล CCTS: Core Component Technical Specification การจัดทำ XML Schema XML NDR: XML Naming and Design Rules

กระบวนการตรวจสอบและประเมินคุณภาพข้อมูล (Data Quality)

กระบวนการตรวจสอบและประเมินคุณภาพข้อมูล (Data Quality) สำนักงาน ป.ป.ท. มีความประสงค์ดำเนินการให้เกิดการตรวจสอบให้ข้อมูลของหน่วยงานมีคุณภาพ ถูกต้อง ครบถ้วน พร้อมใช้อยู่เสมอ โดยยึดตามหลักเกณฑ์การประเมินคุณภาพข้อมูล สำหรับหน่วยงานภาครัฐ (DATA QUALITY ASSESSMENT FRAMEWORK for GOVERNMENT AGENCY) เวอร์ชัน ๑.๐ โดยสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) เพื่อเป็นกรอบและเครื่องมือ ในการประเมินคุณภาพข้อมูลของหน่วยงานภาครัฐในการตรวจสอบและควบคุมการบริหารจัดการข้อมูล เพื่อให้ได้ ข้อมูลที่มีคุณภาพ น่าเชื่อถือ สามารถนำไปใช้ประกอบการวิเคราะห์และตัดสินใจในเชิงนโยบายและการดำเนินงาน ได้อย่างถูกต้องเหมาะสม รวมทั้งสามารถนำไปใช้ประโยชน์เพื่อเพิ่มประสิทธิภาพในการทำงาน เพิ่มคุณค่าในการ ให้บริการภาครัฐ และต่อยอดการพัฒนาของประเทศในมิติต่าง ๆ ได้ ตลอดจนสร้างความเชื่อมั่นให้กับผู้ใช้ข้อมูลภาครัฐ ในมิติต่างๆ โดยมีรายละเอียดการประเมิน ดังนี้

มิติคุณภาพข้อมูล	รายละเอียด
ความถูกต้องและ สมบูรณ์ (Accuracy and Completeness)	ประเมินเรื่องความถูกต้องแม่นยำ แหล่งข้อมูลที่น่าเชื่อถือและมีกระบวนการตรวจสอบ
ความสอดคล้องกัน (Consistency)	ประเมินเรื่องรูปแบบของข้อมูล ความสอดคล้องกัน และมาตรฐานในการจัดทำข้อมูลของหน่วยงาน
ตรงตามความต้องการ ของผู้ใช้ (Relevancy)	ประเมินว่า เป็นข้อมูลที่ผู้ใช้ต้องการหรือเป็นข้อมูลที่จำเป็นต้องทราบ มีความละเอียด เพียงพอต่อการนำไปใช้งาน
ความเป็นปัจจุบัน (Timeliness)	ประเมินเรื่องการเผยแพร่ข้อมูล การปรับปรุงข้อมูลและแผนเรื่อง ระยะเวลา
ความพร้อมใช้ (Availability)	ประเมินความพร้อมใช้ของข้อมูล รวมไปถึงช่องทางในการขอ หรือใช้ข้อมูล

สำนักงาน ป.ป.ท. จึงกำหนดมาตรการประเมินคุณภาพ ตามแนวทางข้างต้น ดังนี้

๑. กำหนดให้มีทีมผู้ประเมินคุณภาพข้อมูล เพื่อทำหน้าที่การประเมินคุณภาพข้อมูลขององค์กร ประกอบด้วยทีมบริกรข้อมูล (Data Stewards Team) ซึ่งเป็นผู้ไม่มีส่วนได้ส่วนเสียกับการดำเนินงานเพื่อให้ไม่เกิดผลประโยชน์ทับซ้อน ดำเนินการตรวจประเมินคุณภาพข้อมูลอย่างน้อยปีละ ๑ ครั้ง ดำเนินการตรวจประเมินคุณภาพข้อมูลตามรายการในแต่ละมิติตาม DQA Checklist และ DQC Checklist

๒. กำหนดให้เจ้าของข้อมูล ดำเนินการประเมินตนเองตาม DQA Self-Assessment ในและนำส่งผลการประเมินให้ทีมผู้ประเมินคุณภาพข้อมูลเพื่อใช้ประกอบการตรวจประเมินคุณภาพข้อมูล

๓. ในการตรวจประเมินของทีมผู้ประเมินคุณภาพข้อมูล ให้ทีมผู้ประเมินคุณภาพข้อมูลดำเนินการประเมินคุณภาพข้อมูลตามเกณฑ์และวิธีการตรวจประเมินตามที่เจ้าของข้อมูลกำหนด และเจ้าของข้อมูลควรกำหนดเกณฑ์และวิธีการตรวจประเมินให้ชัดเจน และชี้แจงให้ทีมผู้ประเมินคุณภาพข้อมูลรับทราบและทำความเข้าใจให้ตรงกันก่อนทำการประเมินคุณภาพข้อมูล

๔. ทีมผู้ประเมินคุณภาพข้อมูล ต้องจัดทำรายงานสรุปผลการตรวจประเมินให้ผู้บริหารรับทราบและดำเนินการตามแผนปฏิบัติการจัดการคุณภาพข้อมูลของหน่วยงานต่อไป

แผนงานการเปิดเผยข้อมูลภาครัฐ
สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

ตามที่ราชกิจจานุเบกษา เผยแพร่ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เมื่อวันที่ ๒๔ มิถุนายน ๒๕๖๓ เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะเพื่อประโยชน์ในการอำนวยความสะดวกแก่ประชาชน ในการเข้าถึงข้อมูล และกำหนดแนวทางและมาตรฐานให้หน่วยงานของรัฐจัดส่งหรือเชื่อมโยงข้อมูลดังกล่าวเปิดเผยแก่ประชาชน ณ ศูนย์กลางข้อมูลเปิดภาครัฐ (Open Government Data of Thailand) ซึ่งสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ (สำนักงาน ป.ป.ท.) ได้ให้ความสำคัญต่อการดำเนินการตามแนวทางธรรมาภิบาลข้อมูลภาครัฐ และการจัดทำข้อมูลเปิดภาครัฐ ในรูแบบสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัลที่สามารถเข้าถึงและใช้ได้อย่างเสรี ไม่จำกัดแพลตฟอร์ม ไม่เสียค่าใช้จ่าย เผยแพร่ ทำซ้ำ หรือใช้ประโยชน์ได้โดยไม่จำกัดวัตถุประสงค์ ซึ่งข้อมูลสามารถนำไป วิเคราะห์ หรือดัดแปลงได้ตามความต้องการ

สำนักงาน ป.ป.ท. จึงได้จัดทำแผนงานสำหรับการจัดทำการเปิดเผยข้อมูลภาครัฐ สำนักงาน ป.ป.ท. ให้สอดคล้องกับแนวทางการตรวจสอบ ปรับปรุงข้อมูล ตามแนวทางธรรมาภิบาลข้อมูลภาครัฐ รวมถึงการพัฒนาระบบเทคโนโลยีสารสนเทศรองรับการปฏิบัติงาน และการรวบรวม วิเคราะห์ เพื่อให้เกิดความถูกต้องของข้อมูล โดยแผนงานและการขับเคลื่อนเพื่อการเปิดเผยข้อมูลสอดคล้องกับการขับเคลื่อนองค์กรตามการมอบอำนาจและการแบ่งกลุ่มภารกิจ ตามคำสั่งสำนักงาน ป.ป.ท. ที่ ๑๕๕/๒๕๖๖ ลงวันที่ ๓๑ พฤษภาคม ๒๕๖๖ โดยมีแผนงาน ดังนี้.

ภารกิจที่ดำเนินการวิเคราะห์และจัดทำเพื่อการเปิดเผยข้อมูล	ระยะเวลาดำเนินการ (ไตรมาส - ปีงบประมาณ)																			
	๒๕๖๖				๒๕๖๗				๒๕๖๘				๒๕๖๙				๒๕๗๐			
กลุ่มภารกิจด้านป้องกันการทุจริต																				
ภารกิจเครือข่ายประชาสังคม																				
ภารกิจส่งเสริมธรรมาภิบาลหน่วยงานรัฐ																				
กลุ่มภารกิจด้านปราบปรามการทุจริต																				
ภารกิจรับเรื่องและบริหารเรื่องร้องเรียน																				
ภารกิจตรวจสอบข้อเท็จจริง																				
ภารกิจบริหารจัดการคดีการทุจริต																				
ภารกิจด้านกฎหมาย																				
กลุ่มภารกิจด้านขับเคลื่อนและกำกับการดำเนินงานนโยบายภาครัฐ																				
ภารกิจขับเคลื่อน ศปท. และการรายงานข้อร้องเรียน																				
ภารกิจบริหารความเสี่ยงภาครัฐ																				
ภารกิจบริหารความเสี่ยงโครงการขนาดใหญ่ภาครัฐ																				
ภารกิจส่งเสริม/ตรวจสอบวิธีปฏิบัติตามกฎหมายภาครัฐ																				
กลุ่มภารกิจด้านอำนวยการ																				
ภารกิจด้านยุทธศาสตร์และแผน																				
ภารกิจด้านงบประมาณ																				
ภารกิจด้านการเงิน																				
ภารกิจด้านบุคลากร																				
ภารกิจด้านตัวชี้วัดและการประเมิน																				
ภารกิจด้านคุณธรรมและความโปร่งใส																				
ภารกิจด้านเทคโนโลยีดิจิทัล																				

คำอธิบาย แผนการปฏิบัติเพื่อเปิดเผยข้อมูล	ข้อมูลระเบียน	ข้อมูลสถิติและอื่นๆ

กฎหมาย ระเบียบ ประกาศ ที่เกี่ยวข้อง

1. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และที่แก้ไขเพิ่มเติม
2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม
3. พระราชบัญญัติมาตรการของฝ่ายบริหารในการป้องกันและปราบปรามการทุจริต พ.ศ. ๒๕๕๑ และที่แก้ไขเพิ่มเติม
4. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
5. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
6. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
7. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔
8. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ พ.ศ. ๒๕๖๓
9. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ พ.ศ. ๒๕๖๓
10. ประกาศคณะกรรมกรพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล ว่าด้วยเรื่อง กรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ พ.ศ. ๒๕๖๕
11. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐและแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐ พ.ศ. ๒๕๖๖
12. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล พ.ศ. ๒๕๖๖