ประกาศกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

เรื่อง นโยบายและแนวทางปฏิบัติธรรมาภิบาลข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล ให้เป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพและตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน รวมทั้งกำหนดให้มีการบริหารจัดการและบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล ประกอบกับคณะกรรมการพัฒนารัฐบาลดิจิทัล ได้ออกประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ เมื่อวันที่ ๑๒ มีนาคม ๒๕๖๓ โดยกำหนดให้หน่วยงานมีธรรมาภิบาลข้อมูลภาครัฐ เพื่อเป็นหลักการและแนวทางในการดำเนินงาน ตามพระราชบัญญัติดังกล่าว

อาศัยอำนาจตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ข้อ ๔ ประกอบมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน เรื่อง นโยบายและแนวทางปฏิบัติธรรมาภิบาลข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน”

ข้อ ๒ นโยบายและแนวทางปฏิบัติธรรมาภิบาลข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน เป็นไปตามเอกสารแนบท้ายประกาศ

ประกาศ ณ วันที่ ๑๙ กันยายน พ.ศ. ๒๕๖๘

(นางสาวนันธิกา ทังสุพานิช)
อธิบดีกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

ด้วยพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะให้เป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพและตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน รวมทั้งกำหนดให้มีการบริหารจัดการและบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล ประกอบกับคณะกรรมการพัฒนารัฐบาลดิจิทัล ได้ออกประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ เมื่อวันที่ 12 มีนาคม 2563 โดยกำหนดให้หน่วยงานมีธรรมาภิบาลข้อมูลภาครัฐ เพื่อเป็นหลักการและแนวทางในการดำเนินงานในการกำกับดูแลข้อมูลภาครัฐในระดับหน่วยงานให้สอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้ข้อมูลมีการจัดเก็บอย่างเป็นระบบ มีคุณภาพ ถูกต้อง ครบถ้วน สนับสนุนการให้บริการแก่ประชาชนอย่างสะดวก รวดเร็ว และมีประสิทธิภาพ กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน จึงเห็นสมควรกำหนดนโยบายธรรมาภิบาลข้อมูล ดังนี้

บทนำ

กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน จัดทำนโยบายธรรมาภิบาลข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานขึ้น เพื่อให้การบริหารจัดการข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานมีธรรมาภิบาล สามารถบูรณาการ เชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกันได้ โดยมีการกำหนดสิทธิ หน้าที่ ความรับผิดชอบในการบริหารจัดการข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน เริ่มตั้งแต่การเก็บรวบรวม การใช้ การประมวลผล รวมถึงการเปิดเผยข้อมูลอย่างเหมาะสม มีประสิทธิภาพ มีคุณภาพ มีความมั่นคง ปลอดภัย สามารถป้องกันภัยคุกคามที่อาจเกิดขึ้นได้ ให้เป็นไปตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

วัตถุประสงค์

1. เพื่อให้มีนโยบายและแนวทางปฏิบัติธรรมาภิบาลข้อมูลสำหรับการบริหารจัดการข้อมูลที่มีความสอดคล้องกับพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 ภายใต้กรอบธรรมาภิบาลข้อมูลภาครัฐของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) รวมถึงกฎหมาย ประกาศ และระเบียบอื่นๆ ที่เกี่ยวข้อง
2. เพื่อกำหนดขอบเขตของธรรมาภิบาลข้อมูล การบริหารจัดการข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ในการจัดเก็บรวบรวมข้อมูล การแบ่งปันข้อมูล การใช้ข้อมูล การตรวจสอบ การประเมินผล และการเปิดเผยข้อมูล
3. เพื่อใช้เป็นแนวทางในการปฏิบัติ พัฒนาและปรับปรุงธรรมาภิบาลข้อมูล รวมถึงการบริหารจัดการข้อมูลให้มีประสิทธิภาพ มีคุณภาพ และมีความมั่นคงปลอดภัย
4. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้แก่ผู้บริหาร บุคลากร และผู้ที่เกี่ยวข้องให้มีความตระหนักถึงความสำคัญของธรรมาภิบาลข้อมูล การบริหารจัดการข้อมูล และปฏิบัติตามอย่างเคร่งครัด

ขอบเขต

ขอบเขตของนโยบายนี้ครอบคลุมวงจรชีวิตของข้อมูล (Data Life Cycle) และกระบวนการธรรมาภิบาลข้อมูล (Data Governance Process) ของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ประกอบด้วยนโยบายผู้บริหารระดับสูงสุดของ พพ. ที่มีการวางกรอบนโยบายให้เป็นไปตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องธรรมาภิบาลข้อมูลภาครัฐ เมื่อวันที่ 12 มีนาคม 2563 ที่สอดคล้องกับสภาพแวดล้อมของ พพ. เพื่อให้คณะกรรมการธรรมาภิบาลข้อมูล ทีมบริกรข้อมูล และเจ้าหน้าที่ของ พพ. ดำเนินการและปฏิบัติตามนโยบายฉบับนี้

คำนิยาม

"พพ." หมายถึง กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

"เจ้าหน้าที่" หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้าง คณะบุคคลหรือผู้ซึ่งมีอำนาจหน้าที่ปฏิบัติงานให้แก่กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

"ธรรมาภิบาลข้อมูลภาครัฐ" หมายถึง การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารข้อมูลของภาครัฐทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานรัฐเป็นไปอย่างถูกต้อง ครบถ้วน และเป็นข้อมูลปัจจุบัน อีกทั้งมาพร้อมกับระบบรักษาความเป็นส่วนบุคคล ที่สามารถเชื่อมโยงแลกเปลี่ยนและบูรณาการระหว่างกันได้

"คณะกรรมการธรรมาภิบาลข้อมูล" หมายถึง คณะกรรมการธรรมาภิบาลข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

"ผู้บริหารระดับสูงสุด" หมายถึง อธิบดีกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

"ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง" หมายถึง รองอธิบดีหรือผู้ที่ได้รับการแต่งตั้งจากผู้บริหารระดับสูงสุด

"ผู้บริหารข้อมูลระดับสูง" หมายถึง รองอธิบดีหรือผู้ที่ได้รับการแต่งตั้งจากผู้บริหารระดับสูงสุด

"ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง" หมายถึง รองอธิบดีหรือผู้ที่ได้รับการแต่งตั้งจากผู้บริหารระดับสูงสุด

"ผู้บริหารจากส่วนงาน" หมายถึง หัวหน้าส่วนราชการระดับ สำนัก/กอง/ศูนย์/กลุ่ม หรือผู้ที่ได้รับมอบหมาย

"หัวหน้าคณะทำงานบริกรข้อมูล" หมายถึง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับการแต่งตั้งจากผู้บริหารระดับสูงสุด

"คณะทำงานบริกรข้อมูล" หมายถึง ทีมบริกรข้อมูลของ พพ. ประกอบด้วย ด้านธุรกิจ ด้านเทคนิค และด้านคุณภาพข้อมูล

"บริกรข้อมูล" หมายถึง เจ้าหน้าที่ ซึ่งได้รับการแต่งตั้งจากคณะกรรมการธรรมาภิบาลข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

"เจ้าของข้อมูล" หมายถึง บุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย ทบทวน และอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล

"ผู้ควบคุมข้อมูล" หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้มีสิทธิในการจัดเก็บข้อมูลและทำลายข้อมูล

"ผู้สร้างข้อมูล" หมายถึง ผู้ใช้ระบบสารสนเทศหรือบริการของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

"ผู้บริหารข้อมูล" หมายถึง ผู้ที่สามารถจัดการข้อมูลกำหนดสิทธิการเข้าถึงข้อมูล

"ผู้ดูแลระบบแม่ข่าย" หมายถึง บุคลากรที่มีหน้าที่ดูแลรับผิดชอบระบบแม่ข่ายของหน่วยงาน

"ผู้ทำลายข้อมูล" หมายถึง บุคลากรที่ได้รับการกำหนดสิทธิจากเจ้าของข้อมูลให้มีสิทธิในการทำลายข้อมูล

"ข้อมูล" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจ ระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

"สารสนเทศ" หมายถึง ข้อมูล ข่าวสาร ในรูปแบบต่าง ๆ เช่น ตัวอักษร ตัวเลข สัญลักษณ์ รูปภาพ เสียง ที่ผ่านกระบวนการประมวลผล และบันทึกไว้อย่างเป็นระบบตามหลักวิชาการในสื่อประเภทต่าง ๆ เช่น หนังสือ วารสาร หนังสือพิมพ์ วีดิทัศน์ ซีดีรอม ฐานข้อมูลอิเล็กทรอนิกส์ ฯลฯ เพื่อนำออกเผยแพร่และใช้ประโยชน์

"พจนานุกรมข้อมูล" หมายถึง ตารางหรือข้อมูลที่ใช้อธิบายรายละเอียดของข้อมูลในแต่ละแถวหรือคอลัมน์

"วงจรชีวิตข้อมูล" หมายถึง ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการเก็บข้อมูลถาวรหรือทำลายข้อมูล

"ชุดข้อมูล" หมายถึง การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล

"บัญชีข้อมูล" หมายถึง เอกสารแสดงรายการของชุดข้อมูล ที่จำแนกแยกแยะ โดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงานของรัฐ

"เมทาดาตา" หมายถึง คำอธิบายชุดข้อมูล ที่ใช้อธิบายชุดข้อมูลหลักหรือกลุ่มของข้อมูลอื่น โดยระบุรายละเอียดแหล่งข้อมูลและคำอธิบายรายละเอียดเกี่ยวกับข้อมูล อาทิ โครงสร้างของข้อมูล เนื้อหาสาระ รูปแบบการจัดเก็บ แหล่งข้อมูล และสิทธิในการเข้าถึงข้อมูล

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) ประกอบด้วย 7 หัวข้อหลัก ได้แก่

1. นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)
2. นโยบายคุณภาพข้อมูล (Data Quality Policy)
3. นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange Policy)
4. มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)
5. นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Data Privacy Policy)
6. นโยบายการเปิดเผยข้อมูล (Open Data Policy)
7. นโยบายการแบ่งปันข้อมูล (Shareable Data Policy)

รายละเอียด มีดังต่อไปนี้

1. นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดแนวทางการดำเนินงานด้านธรรมาภิบาลข้อมูลเนื่องจากการกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูล และให้การบริหารจัดการข้อมูลมีประสิทธิภาพ จึงต้องมีการกำหนด นโยบายที่ระบุอย่างชัดเจน สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง หรือข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง เพื่อให้นโยบายข้อมูลได้ถูกนำมาปฏิบัติอย่างมีประสิทธิภาพและต่อเนื่อง

<u>นโยบาย</u>

1. กำหนดให้มีโครงสร้างการกำกับดูแลข้อมูล พร้อมบทบาทและหน้าที่ความรับผิดชอบ
2. กำหนดกลุ่มบุคคลหรือบุคคลเพื่อเป็นเจ้าของข้อมูลในการบริหารจัดการชุดข้อมูล
3. กำหนดขอบเขตของชุดข้อมูลให้อยู่ในรูปของข้อมูลที่มีโครงสร้าง ข้อมูลกึ่งโครงสร้าง หรือข้อมูลที่ไม่มีโครงสร้าง
4. กำหนดมาตรการ การรักษาความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับการอนุญาต
5. ส่งเสริมการนำระบบเทคโนโลยีสารสนเทศ หรือระบบอัตโนมัติมาใช้ในการจัดทำเมทาดาตา
6. กำหนดให้มีการฝึกอบรม เพื่อสร้างความตระหนักรู้ถึงธรรมาภิบาลข้อมูลภาครัฐอย่างน้อยปีละ 1 ครั้ง
7. กำหนดให้มีการตรวจสอบการปฏิบัติตามนโยบายข้อมูลอย่างน้อยปีละ 1 ครั้ง โดยคณะทำงานบริกรข้อมูล ทำหน้าที่ตรวจสอบ ติดตามผลประเมิน เสนอข้อปรับปรุงและแนวทางแก้ปัญหาที่พบอย่างต่อเนื่อง
8. กำหนดให้มีการตรวจสอบความสอดคล้องระหว่างนโยบายข้อมูลและการดำเนินการใด ๆ ของผู้มีส่วนได้ส่วนเสียอย่างน้อยปีละ 1 ครั้ง
9. กำหนดให้มีการทบทวนนโยบายธรรมาภิบาลข้อมูลทุก 1 ปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ
10. มีมาตรฐานการดำเนินการข้อมูลเปิด (Open Data)

2. นโยบายคุณภาพข้อมูล (Data Quality Policy)

วัตถุประสงค์

เพื่อให้มีการควบคุมคุณภาพข้อมูล สำหรับการนำไปใช้ประโยชน์ในการบริหารงานและการให้บริการประชาชนของ พพ. โดยให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานของ พพ. ตามที่กฎหมายกำหนด โดยข้อมูลที่ได้ทำการจัดเก็บนั้น พพ.จะคำนึงถึงคุณภาพข้อมูล (Data Quality) ในทุกชุดข้อมูล (Dataset) ของ พพ.

นโยบาย

1. กำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน และมีการควบคุมคุณภาพข้อมูลตลอดทั้งวงจรชีวิตข้อมูล (Data Lifecycle) ของข้อมูลที่ตนเองมีหน้าที่รับผิดชอบนั้น
2. กำหนดให้มีข้อกำหนดพื้นฐานของการบริหารจัดการคุณภาพข้อมูล (Data Quality Management) รวมถึงแนวทางการควบคุมและการปรับปรุงอย่างต่อเนื่อง
3. ชุดข้อมูลทุกชุดต้องมีการวัดคุณภาพข้อมูล (Data Quality) ดังต่อไปนี้ ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) และพร้อมใช้งาน (Availability)
4. การกำหนดตัวชี้วัดคุณภาพข้อมูล เช่น ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) และพร้อมใช้งาน (Availability)

3. นโยบายการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange Policy)

วัตถุประสงค์

เพื่อให้การแลกเปลี่ยนข้อมูลทั้งภายในและระหว่างหน่วยงานมีความมั่นคงปลอดภัย และข้อมูลมีคุณภาพสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีวิธีและแนวทางการนำข้อมูลไปเชื่อมโยงและแลกเปลี่ยนกับหน่วยงานภายนอก ให้สอดคล้องกับระเบียบ หลักเกณฑ์ และกฎหมายที่กำหนดบนพื้นฐานของประโยชน์ส่วนรวมเป็นสำคัญ

นโยบาย

1. การแลกเปลี่ยนและการเชื่อมโยงข้อมูลของ พพ. กับหน่วยงานอื่น ให้ดำเนินการโดยเจ้าหน้าที่ที่มีสิทธิให้กระทำการได้
2. กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือช่องทางการติดต่อ
3. กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจนเริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ ให้ดำเนินการตามแนวทางปฏิบัติ การจัดทำบัญชีข้อมูล คุณภาพข้อมูล เชื่อมโยงข้อมูล และการเผยแพร่ข้อมูล
4. กำหนดการคุ้มครองข้อมูลส่วนบุคคลในการแลกเปลี่ยนและเชื่อมโยงข้อมูล และให้เป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy Policy) ของ พพ.
5. กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการแลกเปลี่ยนที่จำเป็นให้ครบถ้วน
6. ทำสัญญาอนุญาตหรือข้อตกลงระหว่างหน่วยงานในการแลกเปลี่ยนข้อมูล การนำข้อมูลไปใช้ เทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

7. บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบได้
8. สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติกระบวนการแลกเปลี่ยน และมาตรฐานตามที่กำหนด

4. มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)

<u>วัตถุประสงค์</u>

เพื่อให้การประมวลผลข้อมูลและการใช้ข้อมูลมีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ รวมถึงวิธีการและแนวทางในการขอข้อมูลจากหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อนำมาใช้ในการประมวลผลและนำมาใช้ ทั้งนี้ การนำข้อมูลมาใช้ให้เป็นไปตามวัตถุประสงค์ตามที่แจ้ง หากนอกเหนือจากเหตุผลดังกล่าวข้างต้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน

<u>นโยบาย</u>

1. ชุดข้อมูลต้องมีการจัดลำดับชั้นความลับของข้อมูล การกำหนดชั้นความลับของข้อมูล และการกำหนดสิทธิ์การเข้าถึง เพื่อให้สอดคล้องกับแนวทางการจัดชั้นความลับของข้อมูล
2. ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม
3. ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล
4. ต้องมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย
5. ให้มีการเปิดเผยเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย
6. สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล
7. การเปิดเผยข้อมูลส่วนบุคคล ให้ดำเนินการตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy Policy) ของ พพ.
8. ต้องมีการทบทวนระดับชั้นความลับข้อมูล อย่างน้อยปีละ 1 ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง

5. นโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Data Privacy Policy)

<u>วัตถุประสงค์</u>

เพื่อเป็นการกำหนดแนวทางในการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลและความเป็นส่วนบุคคล ซึ่งจะต้องสอดคล้องกับนโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

<u>นโยบาย</u>

1. กำหนดให้มีผู้รับผิดชอบการรักษาความมั่นคงและปลอดภัยของข้อมูล
2. กำหนดให้มีการรักษาความลับ (Confidentiality) โดยรักษาข้อมูลตามสภาพของการจัดชั้นความลับและมีการกำหนดสิทธิ์การเข้าถึงข้อมูลนั้น
3. กำหนดให้มีความถูกต้องของข้อมูล (Integrity) โดยให้คงสภาพของข้อมูลหรือการรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความถูกต้องและน่าเชื่อถือ รวมถึงมีการปกป้องข้อมูลให้ปราศจากการถูกเปลี่ยนแปลงโดยผู้ไม่มีสิทธิ์

4. กำหนดให้มีความพร้อมใช้งานของข้อมูล (Availability) โดยให้ข้อมูลต้องพร้อมสำหรับการใช้งานได้เสมอ รวมถึงมีการสำรองข้อมูลไว้เมื่อเกิดภัยพิบัติหรือเหตุการณ์ที่ไม่คาดฝัน หากต้องการใช้ข้อมูล ผู้ใช้งานสามารถใช้ข้อมูลได้ทันทีและใช้ได้อย่างต่อเนื่อง
5. กำหนดให้มีการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy) ตั้งแต่การรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยจะต้องมีการระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจน ห้ามมิให้มี การเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดที่ไม่สอดคล้องกับวัตถุประสงค์ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลนั้น ๆ หรือมีกฎหมายกำหนดให้สามารถกระทำสิ่งนั้นได้
6. กรณีเกิดการรั่วไหลหรือมีการละเมิดข้อมูลส่วนบุคคล ให้ดำเนินการตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Data Privacy Policy) ของ พพ.
7. จัดให้มีการประเมินความมั่นคงปลอดภัยของข้อมูล

6. นโยบายการเปิดเผยข้อมูล (Open Data Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดนโยบายข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้โดยใครก็ตาม แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มาหรือตามเจ้าของข้อมูลกำหนด

<u>นโยบาย</u>

1. กำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการเปิดเผยข้อมูล ได้แก่ กำหนดบุคคลหรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจ ในการเปิดเผยข้อมูล กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการและปรับปรุงการเปิดเผยข้อมูลและกำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้
2. ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม
3. ต้องได้รับการอนุญาตจากเจ้าของข้อมูล (Data Owner) ก่อนการเปิดเผยข้อมูลการนำไปใช้
4. ให้มีการจัดเตรียมข้อมูลที่อยู่ในรูปแบบที่ได้จัดทำไว้เป็นมาตรฐานตามกำหนด และง่ายต่อการนำไปใช้
5. มีการจัดทำเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย
6. ให้มีการคัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ โดยหน่วยงานเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย
7. สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพและเป็นการรักษาคุณภาพของข้อมูล
8. ต้องปฏิบัติตามอย่างเคร่งครัด และป้องกันมิให้มีการเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต

7. นโยบายการแบ่งปันข้อมูล (Shareable Data Policy)

<u>วัตถุประสงค์</u>

เพื่อกำหนดนโยบายข้อมูลที่สามารถนำไปแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐ ภาคเอกชน และภาคประชาชน ให้สามารถเข้าถึงและสามารถนำข้อมูลกลับมาใช้ใหม่ ในขณะที่ยังคงรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล โดยเป็นการจัดเตรียมการเข้าถึงข้อมูลในลักษณะที่มีการควบคุมการเปิดเผยข้อมูล

นโยบาย

1. กำหนดเงื่อนไขให้สอดคล้องตาม “5 Data Sharing Principles” ได้แก่
   1.1 โครงการ (Project) : ข้อมูลจะถูกแบ่งปันเพื่อวัตถุประสงค์ที่เหมาะสมและก่อให้เกิดประโยชน์สาธารณะ
   1.2 คน (People) : ผู้ใช้สิทธิ์ที่เหมาะสมในการเข้าถึงข้อมูล
   1.3 สภาพแวดล้อม (Settings) : ที่เอื้อต่อการแบ่งปันข้อมูลและช่วยลดความเสี่ยงของการใช้งานหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
   1.4 ข้อมูล (Data) : มีการใช้การป้องกันที่เหมาะสมและเป็นสัดส่วนของข้อมูล
   1.5 ผลลัพธ์ (Output) : ผลลัพธ์จากการจัดเตรียมการแบ่งปันข้อมูลได้รับการคุ้มครองอย่างเหมาะสมก่อนที่จะแบ่งปันหรือเผยแพร่ข้อมูลเพิ่มเติม
2. ต้องได้รับการอนุญาตจากเจ้าของข้อมูล (Data Owner) หรือผู้ดูแลข้อมูล ก่อนการแบ่งปันข้อมูลกับผู้ที่ร้องขอ
3. ข้อมูลที่จะทำการแบ่งปันข้อมูลได้ ต้องอยู่ในระดับชั้นความลับ เผยแพร่ในองค์กร (Private), ลับ (Confidential), ลับมาก (Secret)
4. มีการจัดทำเมทาดาตาควบคู่ไปกับข้อมูลที่จะใช้เป็นข้อมูลแบ่งปัน
5. ให้มีการคัดเลือกชุดข้อมูลที่สามารถแบ่งปันได้ โดยหน่วยงานเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย
6. มีการกำหนดข้อตกลงในการแบ่งปันข้อมูลระหว่างผู้ดูแลข้อมูลหรือเจ้าของข้อมูลและหน่วยงานที่ร้องขอหรือแบ่งปันข้อมูล
7. ต้องปฏิบัติตามข้อกำหนดหรือเงื่อนไขอย่างเคร่งครัด และมีบทลงโทษหากมีการฝ่าฝืนโดยไม่ได้รับอนุญาต

การทบทวนนโยบายข้อมูล

กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน โดยคณะกรรมการธรรมาภิบาลข้อมูลและทีมบริกรข้อมูลต้องร่วมกันดำเนินการทบทวนนโยบายธรรมาภิบาลข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานเมื่อมีการเปลี่ยนแปลงที่สำคัญหรือตามความเหมาะสม

แนวทางปฏิบัติธรรมาภิบาลข้อมูล ของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

ส่วนที่ 1
บทนำ

ในยุคดิจิทัลที่ข้อมูลเป็นทรัพยากรที่สำคัญในการพัฒนาประเทศ การจัดการข้อมูลของภาครัฐอย่างมีประสิทธิภาพและโปร่งใสเป็นสิ่งจำเป็นอย่างยิ่ง กรอบธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Framework) เป็นแนวทางที่ช่วยให้หน่วยงานรัฐสามารถบริหารจัดการข้อมูลได้อย่างเป็นระบบ ปลอดภัย และสอดคล้องกับหลักการที่ดี

กรอบธรรมาภิบาลข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานนี้ มีเป้าหมายเพื่อให้การได้มาซึ่งข้อมูล การจัดเก็บ การใช้งาน และการเผยแพร่ข้อมูล เป็นไปอย่างถูกต้อง ครบถ้วน เป็นปัจจุบัน และมั่นคงปลอดภัย จะช่วยให้การตัดสินใจและการวางนโยบายของภาครัฐมีประสิทธิภาพมากขึ้น กรอบธรรมาภิบาลข้อมูลภาครัฐช่วยให้มั่นใจได้ว่าข้อมูลจะถูกจัดการอย่างเหมาะสมและเป็นไปตามมาตรฐานที่กำหนด ทำให้การตัดสินใจมีความโปร่งใสและตรวจสอบได้ เพื่อให้ข้อมูลมีคุณภาพ และมีการเชื่อมโยงภายใต้กรอบธรรมาภิบาลข้อมูลโดยมีคณะกรรมการธรรมาภิบาลข้อมูลทำหน้าที่กำหนดยุทธศาสตร์ และเป้าหมาย กำหนดขอบเขตและตรวจสอบสภาพแวดล้อมธรรมาภิบาลข้อมูล รวมทั้งกำหนดนิยามและมาตรฐานของข้อมูล ดังแสดงในรูปที่ 1

รูปที่ 1 กรอบธรรมาภิบาลข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน

กรอบธรรมาภิบาลข้อมูลของกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงานประกอบด้วย นิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล (Definition and Rules) โครงสร้างธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Structure) และกระบวนการธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Processes)

โดยบุคคลต่าง ๆ ที่เกี่ยวข้องกับโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ จะถูกแต่งตั้งโดยผู้บริหารระดับสูงของหน่วยงาน เพื่อทำหน้าที่กำหนดยุทธศาสตร์และเป้าหมาย ตรวจสอบสภาพแวดล้อมของธรรมาภิบาลข้อมูล นิยามความหมายและขอบเขตของข้อมูล กำหนดกฎเกณฑ์และนโยบายข้อมูล และดำเนินการตรวจสอบการปฏิบัติตามกฎเกณฑ์และนโยบายการบริหารจัดการข้อมูล

วิสัยทัศน์ของธรรมาภิบาลข้อมูล

เป็นองค์กรที่มีกรอบธรรมาภิบาลข้อมูล การบริหารจัดการข้อมูลที่มีความปลอดภัยและมีประสิทธิภาพ

พันธกิจธรรมาภิบาลข้อมูล

1. มีโครงสร้างองค์กรที่สอดรับกับธรรมาภิบาลข้อมูล
2. ทำให้ข้อมูลมีคุณภาพและมีความน่าเชื่อถือในการใช้งานทั้งภายในและภายนอกองค์กร
3. มีกระบวนการและตัวชี้วัดในด้านข้อมูลในองค์กร
4. มีการเสริมสร้างความรู้ความเข้าใจด้านการบริหารจัดการข้อมูลกับบุคลากรทุกระดับ
5. ใช้เทคโนโลยีดิจิทัลมาสนับสนุนการทำงานด้านธรรมาภิบาลข้อมูลอย่างเต็มประสิทธิภาพ

เป้าหมายธรรมาภิบาลข้อมูล

1. มีคณะกรรมการธรรมาภิบาลข้อมูลและผู้บริหารข้อมูลระดับสูง
2. มีการกำหนดนโยบายด้านข้อมูลในแต่ละส่วนงานให้ครอบคลุมด้านคุณภาพข้อมูล การเชื่อมโยงข้อมูล และความมั่นคงปลอดภัยข้อมูล
3. บุคลากรมีความรู้ความเข้าใจด้านการจัดการข้อมูลที่ดีเพื่อทำให้องค์กรไปสู่เป้าหมายร่วมกัน
4. มีความร่วมมือด้านการแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก
5. มีมาตรฐานการดำเนินการข้อมูลเปิด (Open data)
6. มีมาตรฐานการดำเนินการข้อมูลแบ่งปัน (Shareable data)

ยุทธศาสตร์ธรรมาภิบาลข้อมูล

1) กำหนดโครงสร้างธรรมาภิบาลข้อมูล
   1.1) จัดตั้งคณะกรรมการธรรมาภิบาลข้อมูลและผู้บริหารข้อมูลระดับสูง
   1.2) มีการระบุหน้าที่ความรับผิดชอบของแต่ละส่วนงานด้านข้อมูล
   1.3) มีการระบุหน้าที่ความรับผิดชอบของหัวหน้าคณะทำงานบริกรข้อมูลและบริกรข้อมูล
2) สร้างมาตรฐานธรรมาภิบาลข้อมูล
   2.1) มีการกำหนดมาตรฐานเชิงธุรกิจและเทคโนโลยีในแต่ละส่วนงานให้ครอบคลุมด้านคุณภาพข้อมูล การเชื่อมโยงข้อมูล และความมั่นคงปลอดภัยข้อมูล
   2.2) มีการกำหนดกระบวนการ ผู้รับผิดชอบ ข้อตกลงการให้บริการ และตัวชี้วัดในแต่ละส่วนงาน รวมถึงเกณฑ์การประเมินให้ครอบคลุมด้านคุณภาพข้อมูล การเชื่อมโยงข้อมูล และความมั่นคงปลอดภัยข้อมูล
   2.3) มีการดำเนินการเพื่อรองรับมาตรฐานข้อมูลเปิดภาครัฐในอนาคต
3) พัฒนาบุคลากรด้านธรรมาภิบาลข้อมูล
   3.1) มีการสื่อสารองค์กรด้านการจัดการข้อมูลที่ดี
   3.2) การฝึกอบรมเพื่อเสริมสร้างความรู้และทักษะของบุคลากร

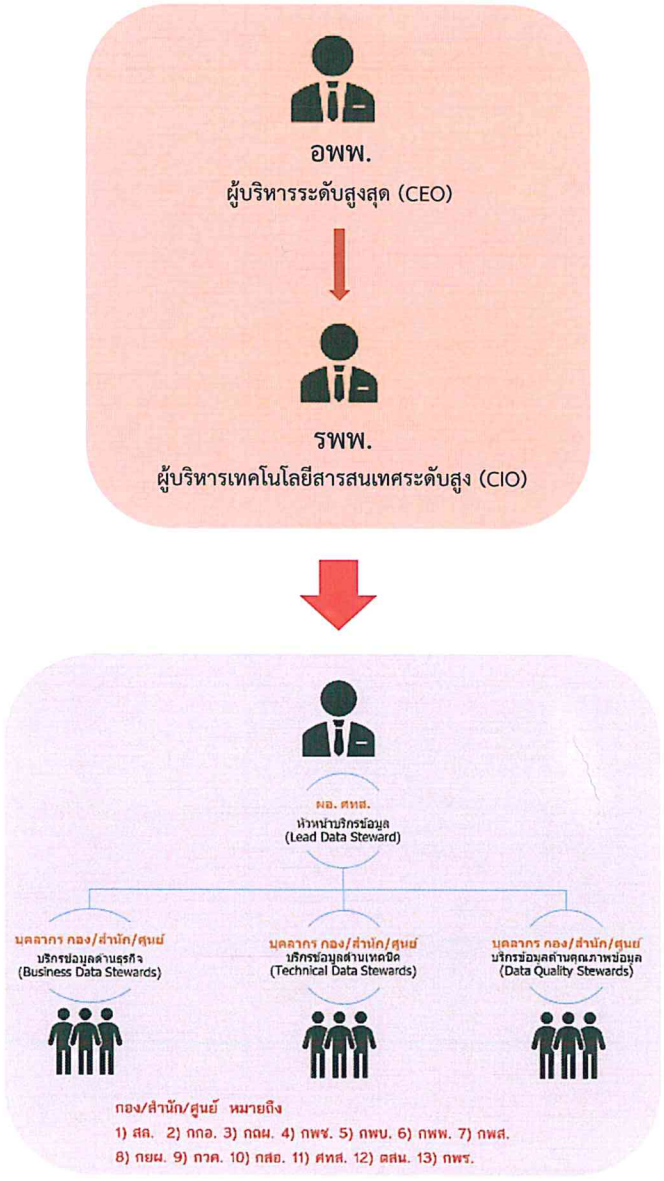
ส่วนที่ 2
โครงสร้างธรรมาภิบาลข้อมูล

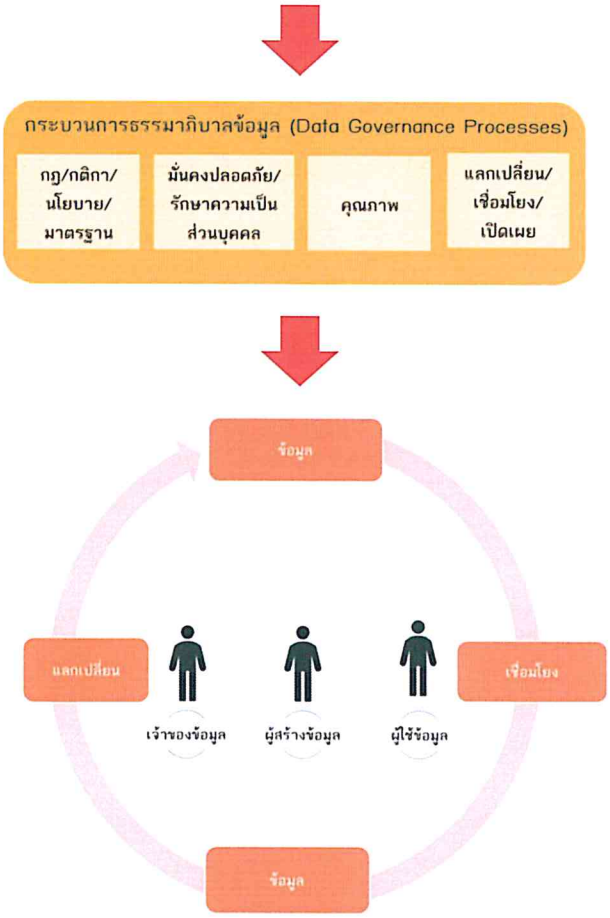
วัตถุประสงค์

กำหนดโครงสร้างธรรมาภิบาลข้อมูลเพื่อแสดงลำดับขั้นระหว่างกลุ่มบุคคลที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล และแสดงถึงสิทธิ์ในการใช้งานตามลำดับขั้นแนวปฏิบัติ โดยแบ่งออกเป็น 3 ส่วน ประกอบด้วย

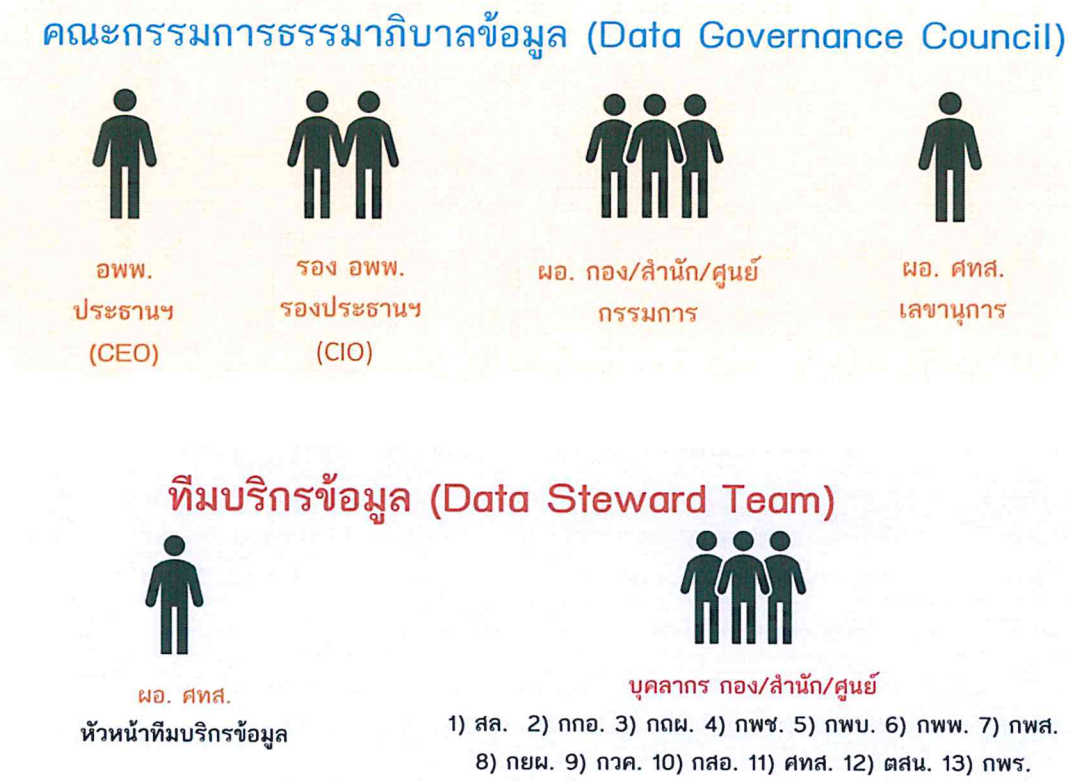
1. คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)
2. คณะทำงานบริกรข้อมูล (Data Steward Team)
3. ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders)

โครงสร้างธรรมาภิบาลข้อมูลดังแสดงในรูปที่ 2 และรูปที่ 3 ส่วนตารางที่ 1 เป็นการกำหนดบทบาทและหน้าที่ความรับผิดชอบตามตำแหน่งต่างๆ ภายในโครงสร้างธรรมาภิบาลข้อมูล ของ พพ.





รูปที่ 2 แสดงโครงสร้างธรรมาภิบาลข้อมูลของ พพ.



รูปที่ 3 แสดงโครงสร้างธรรมาภิบาลข้อมูลตามตำแหน่งของ พพ.

ตารางที่ 1 บทบาทและหน้าที่ความรับผิดชอบตามโครงสร้างธรรมาภิบาลข้อมูล

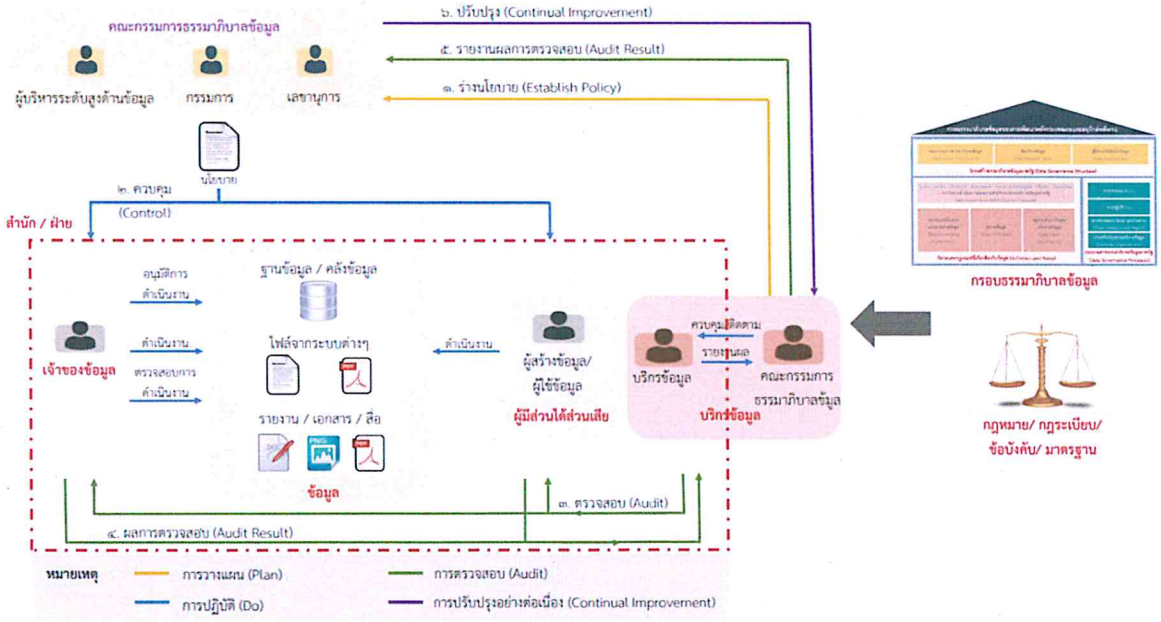
บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO)	อธิบดีกรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน	ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการภายในคณะกรรมการกำกับดูแลข้อมูล
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) หรือผู้บริหารข้อมูลระดับสูง (Chief Data Officer) (CIO และ CDO เป็นคนเดียวกันได้)	รองอธิบดีหรือผู้ที่ได้รับการแต่งตั้งจากผู้บริหารระดับสูงสุด	• วิเคราะห์ข้อมูลของหน่วยงานเพื่อสร้างและส่งมอบ เทคโนโลยี เครื่องมือ แนวทาง และวิธีการในการทำให้ข้อมูลของหน่วยงานมีคุณค่า และเกิดประโยชน์สูงสุดต่อองค์กร เพื่อขยายผลต่อไปให้เกิดผลสัมฤทธิ์ ในการส่งเสริมให้องค์กรใช้ข้อมูลได้อย่างถูกต้องและมีประสิทธิภาพ • วิเคราะห์ข้อมูลร่วมกับผู้บริหารส่วนอื่น ๆ เพื่อจัดทำยุทธศาสตร์และดำเนินการกำกับดูแลข้อมูลให้มีคุณภาพ และการควบคุมอื่นๆ เพื่อรักษาความสมบูรณ์ของข้อมูลขององค์กร
ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (Chief Security Officer: CSO)	รองอธิบดีหรือผู้ที่ได้รับการแต่งตั้งจากผู้บริหารระดับสูงสุด	• บริหารข้อมูลให้มีความปลอดภัย และเพียงพอสำหรับการทำงาน

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
		• ทำให้เกิดการเชื่อมต่อระหว่างหน่วยงานภาครัฐ รวมทั้งปรับปรุงความมั่นคงทางกายภาพ และความปลอดภัยด้านเทคโนโลยีให้มากขึ้น • ทำงานร่วมกับผู้บริหารอื่น ๆ ในการตัดสินใจเกี่ยวกับ ลำดับความสำคัญของความต้องการด้านความปลอดภัย • กำหนดเป้าหมายและวัตถุประสงค์ของการป้องกันหน่วยงาน เพื่อให้สอดคล้องกับแผนกลยุทธ์ของหน่วยงาน • ดูแลเครือข่ายของคณะกรรมการ ผู้บริหาร และเจ้าหน้าที่รักษาความปลอดภัย • ทำงานร่วมกับหน่วยงานด้านความมั่นคง และหน่วยงานรักษาความปลอดภัยอื่นๆ
คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)	ผู้อำนวยการ กอง/สำนัก/ศูนย์ หรือผู้ที่ได้รับมอบหมาย	• ให้คำแนะนำ ข้อเสนอแนะ และวิพากษ์ประเด็นต่างๆ ที่เกี่ยวข้องกับการบริหารจัดการข้อมูลในส่วนงานที่ตนเองรับผิดชอบและส่วนงานอื่นๆ ที่เกี่ยวข้อง • ร่วมกำหนดนโยบายธรรมาภิบาลข้อมูล • สื่อสารไปยังทีมงานภายใต้ส่วนงานที่ตนรับผิดชอบ เพื่อให้บุคลากรอื่น ๆ ในองค์กร ได้รับทราบถึงนโยบายและแนวปฏิบัติของธรรมาภิบาลข้อมูล
คณะทำงานบริกรข้อมูล (Data Steward Team)		
หัวหน้าคณะทำงานบริกรข้อมูล (Lead Data Steward)	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับการแต่งตั้งจากผู้บริหารระดับสูงสุด และควรเป็นเลขานุการของคณะกรรมการธรรมาภิบาลข้อมูล	• ควบคุมและสั่งการภายในทีมบริกรข้อมูล
บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) (1) บริกรข้อมูลด้านการกำกับมาตรฐานงานดิจิทัลสารสนเทศ	บุคลากร กอง/สำนัก/ศูนย์ (บริกรข้อมูลด้านธุรกิจ และบริกรข้อมูลด้านคุณภาพข้อมูล) บุคลากร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (บริกรข้อมูลด้านเทคนิค)	• กำหนดมาตรฐาน แผนงาน และการให้บริการ รวมถึงแนวทางในการใช้โครงข่ายพื้นฐานเพื่อสนับสนุน เทคโนโลยีสารสนเทศขององค์กร • ควบคุม กำกับ ตรวจสอบ และติดตามการปฏิบัติตามนโยบายข้อมูล ตรวจสอบคุณภาพ ตรวจสอบความมั่นคงปลอดภัยของข้อมูล วิเคราะห์ผลจากการตรวจสอบ • ให้ข้อเสนอแนะมาตรฐาน วิเคราะห์ข้อมูล และเชิงเทคนิค และการนำไปประยุกต์ใช้บริหารข้อมูลสารสนเทศ และการปฏิบัติตามนโยบายข้อมูลงานระบบสารสนเทศ • ให้คำปรึกษาและแนะนำหรือ ฝึกอบรม การใช้คอมพิวเตอร์ และการใช้โปรแกรมพัฒนาบุคลากรภาครัฐด้านเทคโนโลยีสารสนเทศและการสื่อสาร • พัฒนาระบบเครือข่าย รวมทั้งเฝ้าระวัง ป้องกัน และแก้ไขภัยคุกคามที่อาจเกิดขึ้น จากระบบงานเทคโนโลยีสารสนเทศ

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
(หัวหน้ากลุ่มพัฒนาระบบสารสนเทศ และหัวหน้ากลุ่มเทคโนโลยีสารสนเทศ) (2) บริกรข้อมูลด้านวิเคราะห์ข้อมูลและพัฒนาระบบดิจิทัล (หัวหน้ากลุ่มพัฒนาระบบสารสนเทศ) (3) บริกรข้อมูลด้านโครงสร้างพื้นฐานดิจิทัล (หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ)		• ประสานงานและสนับสนุนด้านเทคโนโลยีสารสนเทศ โดยดำเนินการบริหารโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศขององค์กรทั้งที่เป็นศูนย์กลางหรือที่ใช้ร่วมกัน • สำรวจ เก็บรวบรวมข้อมูล ติดตามความเคลื่อนไหวของสถานการณ์ และแนวโน้มการพัฒนาด้านดิจิทัล • บำรุงรักษางานโครงสร้างพื้นฐานสารสนเทศให้พร้อมใช้งานตลอดเวลา แก้ไข และช่วยเหลือผู้ใช้งานระบบสารสนเทศในองค์กร • รายงานผลลัพธ์การตรวจสอบไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ ให้ทราบ
ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)		• มีส่วนร่วมในการดำเนินงานด้านธรรมาภิบาลข้อมูลภาครัฐในหน่วยงาน • แจ้งประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพ การรักษาความเป็นส่วนบุคคล และความมั่นคงปลอดภัยของข้อมูล • ให้ข้อคิดเห็น ข้อเสนอแนะแก่ทีมบริกรข้อมูลและคณะกรรมการธรรมาภิบาลข้อมูล
เจ้าของข้อมูล (Data Owners) และ/หรือ ผู้ครอบครองข้อมูล (Data Processor)	หัวหน้าส่วนราชการระดับกอง/สำนัก/ศูนย์ หรือผู้ที่ได้รับมอบหมาย	• ตรวจสอบดูแลข้อมูลโดยตรง เพื่อสร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลมีความสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบหรือกฎหมาย โดยเจ้าของข้อมูลจะทำการทบทวนและอนุมัติการดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูล
ทีมบริหารจัดการข้อมูล (Data Management Team) (1) สถาปนิกข้อมูล (Data Architects) (2) นักจัดการฐานข้อมูล (Database Administrators) (3) นักวิเคราะห์ข้อมูล (Data Analysts)	บุคลากร กอง/สำนัก/ศูนย์	มีหน้าที่หลักในการบริหารจัดการข้อมูลให้สอดคล้องกับการบริหารจัดการข้อมูล และดูแลรักษาข้อมูลในระบบสารสนเทศของหน่วยงานและสนับสนุนกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐ • ทำหน้าที่ออกแบบและจัดทำสถาปัตยกรรมข้อมูล (Data Architecture) จำลองและการออกแบบข้อมูล (Data Modeling and Design) และกำหนดโครงสร้าง (infrastructure) สำหรับจัดการกับข้อมูล • ทำหน้าที่จัดเก็บและการดำเนินการกับข้อมูล (Data Storage and Operations) รวมถึงการดูแล บำรุงรักษา ปรับปรุงประสิทธิภาพการทำงาน และวางแผนการจัดเก็บข้อมูล • ทำหน้าที่นำข้อมูลมาวิเคราะห์ หรือแก้ปัญหาจากสิ่งที่ผิดปกติ โดยใช้ประสบการณ์และหลักสถิติ รวมถึงใช้โมเดลหรือเครื่องมือในการทำรายงาน เพื่อสรุปข้อมูลสำหรับใช้ในการตัดสินใจ

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
(4) นักวิทยาการข้อมูล (Data Scientists)		• ทำหน้าที่นำข้อมูลจากหลาย ๆ แหล่ง และแปลงข้อมูล เพื่อหารูปแบบ และความสัมพันธ์ของข้อมูล รวมถึงสร้างแบบจำลองและดำเนินการกับข้อมูลด้วยวิธีการต่าง ๆ เช่น Machine Learning หรือเขียนโปรแกรม เพื่อทำนายมุมมองหรือการคาดการณ์ในอนาคต
ผู้สร้างข้อมูล (Data Creator)	ข้าราชการ พนักงานราชการ ลูกจ้าง คณะบุคคล หรือผู้ซึ่งมีอำนาจหน้าที่ปฏิบัติงานให้แก่กรมพัฒนาพลังงานทดแทนและอนุรักษ์พลังงาน ทำหน้าที่ในการนำเข้าข้อมูลหรือกรอกข้อมูล	ทำหน้าที่ในการบันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้ สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ นอกจากนี้ยังมีหน้าที่ ในการทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย
ผู้ใช้งานข้อมูล (Data User)	• ผู้บริหารและข้าราชการ พพ. • ผู้ใช้บริการของ พพ. • ผู้มีส่วนได้ส่วนเสียอื่นๆ ที่เกี่ยวข้องกับ พพ.	ทำหน้าที่ในการนำข้อมูลไปใช้งานทั้งในระดับบริหารและระดับปฏิบัติงาน และสนับสนุนการกำกับดูแลข้อมูลภาครัฐโดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริกรข้อมูล

ส่วนขั้นตอนการดำเนินงานภายใต้กรอบธรรมาภิบาลข้อมูล ดังแสดงในรูปที่ 4



รูปที่ 4 ขั้นตอนการดำเนินงานภายใต้กรอบธรรมาภิบาลข้อมูล

ส่วนที่ 3
การเชื่อมโยงข้อมูล

วัตถุประสงค์

เพื่อกำหนดมาตรฐาน กระบวนการ บุคลากร หน้าที่และความรับผิดชอบ และเทคโนโลยีที่ พพ. ต้องปฏิบัติในการเชื่อมโยงข้อมูล (Data Integration)

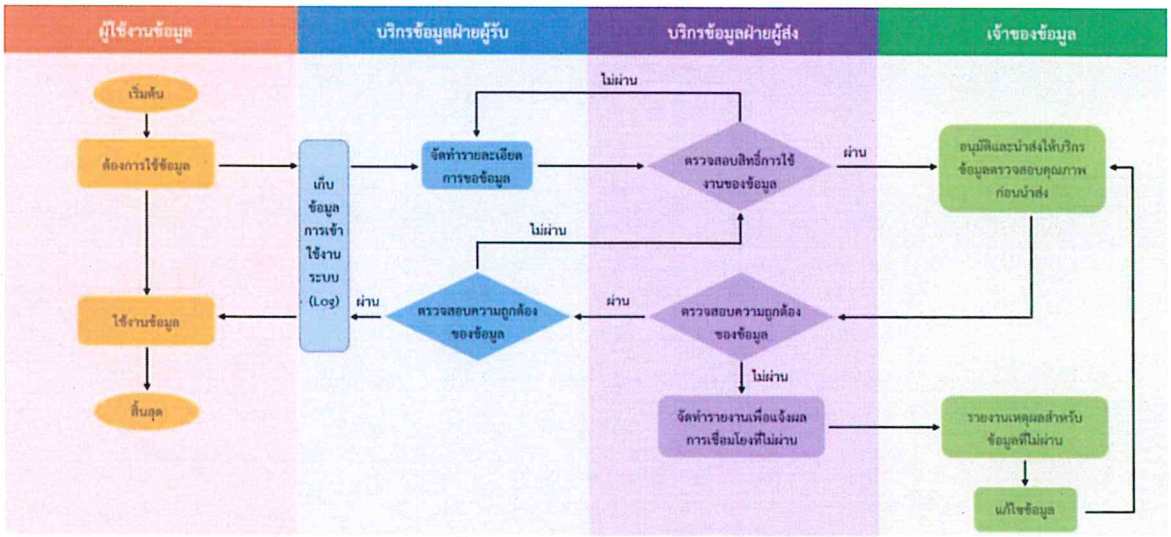
แนวปฏิบัติ

1. บริกรข้อมูลฝ่ายผู้ส่งจะเป็นผู้รับเรื่อง เมื่อฝ่ายผู้รับพบปัญหาใดๆ เกี่ยวกับการเชื่อมโยงข้อมูล หรือคุณภาพข้อมูลที่ส่งไปบริกรข้อมูลของทั้งสองฝ่ายทำหน้าที่ในการตรวจสอบความถูกต้องของข้อมูล

2. บริกรข้อมูลฝ่ายผู้ส่งมีหน้าที่ในการรับเรื่องปัญหาที่เกิดขึ้นในการเชื่อมโยงข้อมูล และประสานกับผู้ที่เกี่ยวข้องต่อไป

3. จะต้องมีการจัดทำเอกสารมาตรฐานการเชื่อมโยงข้อมูล ซึ่งประกอบด้วย ชื่อชุดข้อมูลวันและเวลาในการส่งออกข้อมูล และวันและเวลาที่ผู้รับได้รับข้อมูล โดยต้องมีการจัดเก็บบันทึกประวัติการส่ง การรับและการเชื่อมโยงข้อมูลในแต่ละสำนัก/กอง/ศูนย์/กลุ่ม

4. การตรวจสอบข้อมูลจะต้องอ้างอิงตามคำอธิบายชุดข้อมูล (Metadata) และข้อมูลอ้างอิงของชุดข้อมูลนั้น



รูปที่ 5 กระบวนการเชื่อมโยงระหว่างสำนัก/กอง/ศูนย์/กลุ่มของ พพ.

ส่วนที่ 4
การจัดชั้นความลับของข้อมูล

วัตถุประสงค์

เพื่อกำหนดมาตรฐาน กระบวนการ บุคลากร หน้าที่และความรับผิดชอบ และเทคโนโลยีที่ พพ. ต้องปฏิบัติในการจัดชั้นความลับของข้อมูล

แนวปฏิบัติ

1. ทุกชุดข้อมูลต้องมีการจัดลำดับชั้นความลับของข้อมูล ดังต่อไปนี้

1.1 ระดับที่ 1 ข้อมูลสาธารณะ ได้แก่ ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ

1.2 ระดับที่ 2 ข้อมูลใช้ภายใน ได้แก่ ข้อมูลสำหรับใช้ในการดำเนินกิจการภายในของหน่วยงาน ไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาตจากเจ้าของข้อมูล

1.3 ระดับที่ 3 ข้อมูลส่วนบุคคล ได้แก่ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

1.4 ระดับที่ 4 ข้อมูลความลับทางราชการ ได้แก่ ข้อมูลข่าวสารตามมาตรา 14 หรือมาตรา 15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่มีคำสั่งไม่ให้มีการเปิดเผยและอยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐหรือที่เกี่ยวกับเอกชน ซึ่งมีการกำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือชั้นลับที่สุด ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานของรัฐและประโยชน์แห่งรัฐประกอบกัน

1.5 ระดับที่ 5 ข้อมูลความมั่นคง ได้แก่ ข้อมูลภายใต้กรอบความมั่นคงแห่งชาติ หรือภาวะที่ประเทศปลอดจากภัยคุกคามต่อเอกราช ส่งผลต่อความสงบเรียบร้อย เสถียรภาพความเป็นปึกแผ่น ตลอดจนปลอดภัยจากภัยคุกคาม สอดคล้องตามเป้าหมายของนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ

2. การจัดลำดับชั้นความลับข้อมูลดำเนินการโดยทีมบริกรข้อมูล และได้รับอนุมัติโดยคณะกรรมการธรรมาภิบาลข้อมูล

3. ในการประชุมคณะกรรมการธรรมาภิบาลข้อมูล จำเป็นต้องบรรจุวาระเกี่ยวกับการทบทวน ระดับชั้นความลับข้อมูล อย่างน้อยปีละ 1 ครั้ง

4. ทุกฟิลด์ในแต่ละชุดข้อมูลถือว่ามีระดับชั้นความลับเท่ากัน สำหรับชุดข้อมูลที่มีระดับความลับเป็น ระดับที่ 2 ถึง ระดับที่ 5 จำเป็นต้องระบุสิทธิในการเข้าถึงข้อมูลภายในองค์กรด้วย

5. การเผยแพร่ข้อมูลระดับที่ 1 ต้องได้รับการอนุมัติจากผู้บริหารข้อมูลระดับสูง

6. ข้อมูลระดับที่ 2 เป็นต้นไปจะต้องมีกระบวนการในการร้องขอข้อมูล

7. บุคคลเจ้าของข้อมูลมีหน้าที่ร่วมพิจารณาและรับทราบการร้องขอข้อมูลส่วนบุคคล

8. เจ้าของข้อมูลมีหน้าที่พิจารณาอนุมัติการร้องขอข้อมูลร่วมกับบริกรข้อมูล และตรวจสอบ ทบทวนการจัดลำดับชั้นความลับข้อมูล

9. บริกรข้อมูล มีหน้าที่ตรวจสอบการใช้งานข้อมูลสาธารณะและประเมินผลกระทบของการคุ้มครองข้อมูล (Data Protection Impact Assessment: DPIA)

10. เจ้าของข้อมูลทำหน้าที่อนุมัติการร้องขอข้อมูลร่วมกับบริกรข้อมูล

11. ในกรณีที่ผู้ร้องขอข้อมูลไม่ได้มีสิทธิตามสิทธิการเข้าถึงข้อมูลจำเป็นต้องดำเนินการตามกระบวนการดังต่อไปนี้

11.1 ข้อมูลส่วนบุคคล ต้องมีการร้องขอผ่านส่วนงานที่บุคคลนั้นสังกัด โดยแจ้งวัตถุประสงค์ให้ชัดเจน โดยบุคคลเจ้าของข้อมูล และบริกรข้อมูลของฝ่ายทรัพยากรบุคคลต้องรับทราบและมีสิทธิที่จะปฏิเสธการร้องขอนั้นเว้นแต่จะมีประกาศของ พพ. รองรับ

11.2 ข้อมูลความลับทางราชการ ต้องมีการร้องขอผ่านส่วนงานที่เป็นเจ้าของข้อมูล โดยเจ้าของข้อมูลและบริกรข้อมูลแต่ละกอง/ศูนย์/กลุ่มงานต้องพิจารณาร่วมกัน ถ้าเป็นข้อมูลที่มีความอ่อนไหวหรือมีความเสี่ยงต้องได้รับการอนุมัติโดยคณะกรรมการธรรมาภิบาลข้อมูล

11.3 ข้อมูลความมั่นคง ต้องมีการร้องขอผ่านส่วนงานที่เป็นเจ้าของข้อมูล โดยต้องได้รับการอนุมัติจากคณะกรรมการธรรมาภิบาลข้อมูลเท่านั้น

12. ระดับชั้นความลับข้อมูลจะต้องถูกระบุไว้ในคำอธิบายชุดข้อมูล (Metadata)

13. การร้องขอข้อมูลต้องมีการเก็บบันทึกด้วย

ส่วนที่ 5
กระบวนการจัดการข้อมูลตามวงจรชีวิตข้อมูล

วัตถุประสงค์

เพื่อให้การบริหารจัดการชุดข้อมูลของ พพ. มีประสิทธิภาพและเกิดประสิทธิผลในการนำไปใช้ประโยชน์

แนวปฏิบัติ

1. การสร้างข้อมูล (Create)

1.1 กำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน หรือสร้างข้อมูลตามมาตรฐานที่เกี่ยวข้อง

1.2 กำหนดหน้าที่ความรับผิดชอบในการนำเข้าข้อมูล และการเข้าถึงข้อมูล

1.3 กำหนดสิทธิการเข้าถึงข้อมูล วิธีและเครื่องมือที่ใช้ในการเข้าถึงข้อมูล

1.4 กำหนดระยะเวลาในการทบทวนสิทธิและวิธีในการเข้าถึงข้อมูล

1.5 ให้หน่วยงานที่สร้างข้อมูล ตรวจสอบและบันทึกข้อมูลตั้งต้นให้ถูกต้อง ครบถ้วน ตรงกับข้อเท็จจริง โดยมีการบันทึกข้อมูลและจัดเก็บตามขั้นตอนการรักษาความปลอดภัย

2. การรวบรวมและการจัดเก็บข้อมูล (Collect/Store)

2.1 การรวบรวมและจัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน และจัดทำเมทาดาตาสำหรับชุดข้อมูลที่มีการจัดเก็บอยู่ในฐานข้อมูล

2.2 กรณีเป็นการจัดเก็บข้อมูลส่วนบุคคล ต้องมีการแจ้งหรือขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคลและเลือกใช้ฐานกฎหมายตามความเหมาะสมเพื่อให้เป็นไปตามนโยบายข้อมูลส่วนบุคคลขององค์กร

2.3 กำหนดกระบวนการทดสอบข้อมูลที่จัดเก็บให้มีความถูกต้องและครบถ้วน

2.4 กำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลต่าง ๆ อย่างเหมาะสม

2.5 กำหนดความต้องการหรือคุณลักษณะของระบบจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัย และคุณภาพของข้อมูล

2.6 กำหนดการสำรองข้อมูลหากเกิดเหตุฉุกเฉิน เพื่อให้สามารถใช้งานข้อมูลได้อย่างต่อเนื่อง

3. การคัดแยกข้อมูล (Classify)

3.1 กำหนดเงื่อนไขในการเผยแพร่ข้อมูลสำหรับผู้ใช้ภายในและภายนอกให้ชัดเจน

3.2 ลดความยุ่งยากและซับซ้อนในการเปิดเผยข้อมูลให้เหลือน้อยที่สุด

4. การประมวลผลหรือใช้ข้อมูล (Process/Use)

4.1 กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และสื่อสารให้ผู้ที่เกี่ยวข้องทราบ

4.2 การประมวลข้อมูลที่เป็นความลับ ให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ที่ประกาศไว้อย่างเคร่งครัด

4.3 กำหนดกระบวนการ และเทคโนโลยีในการแลกเปลี่ยน/เชื่อมโยงข้อมูลให้ชัดเจน ตั้งแต่ ขั้นตอนการเตรียมการ เริ่มดำเนินการ ระหว่างดำเนินการ และสิ้นสุดการดำเนินการให้เป็นไปตามมาตรฐานที่เกี่ยวข้อง

5. การปกปิดหรือเปิดเผยข้อมูล (Concealment/Disclosure)

5.1 การกำหนดชั้นความลับของข้อมูลต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ ความเป็นส่วนบุคคล ฯลฯ และต้องตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้น ๆ เพื่อเป็นการรักษาคุณภาพและความมั่นคงปลอดภัยของข้อมูล

5.2 ให้มีการเปิดเผยคำอธิบายชุดข้อมูล (Metadata) ควบคู่ไปกับข้อมูลที่เปิดเผย

5.3 ให้มีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

5.4 กำหนดระยะเวลาในการทบทวนสิทธิและวิธีการในการเข้าถึงข้อมูล

5.5 ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบายหรือแนวปฏิบัติ

5.6 การเปิดเผยข้อมูลต้องอยู่ภายใต้ฐานกฎหมาย หรือได้รับความยินยอมจากเจ้าของข้อมูล

5.7 ต้องมีการป้องกันมิให้มีการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

6. การตรวจสอบข้อมูล (Inspect)

6.1 กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของระบบที่ใช้ในการให้บริการหรือระบบงานสารสนเทศอย่างน้อยปีละ 1 ครั้ง

6.2 ต้องสามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมเป็นไปตามแนวทางที่กำหนดไว้

6.3 หากพบว่าข้อมูลที่จัดเก็บไม่ถูกต้องให้แจ้งเจ้าของข้อมูลเพื่อปรับปรุงแก้ไข

7. การทำลายข้อมูล (Destroy)

7.1 กำหนดระยะเวลาในการจัดเก็บข้อมูลที่เหมาะสมกับข้อมูลแต่ละประเภท

7.2 กำหนดอำนาจอนุมัติสิทธิและยืนยันตัวบุคคลในการทำลายข้อมูล

7.3 ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ผู้ควบคุมข้อมูลหรือหน่วยงานที่จัดเก็บต้องดำเนินการให้เร็วที่สุด ทั้งนี้ต้องไม่ขัดต่อข้อตกลงระหว่างเจ้าของข้อมูลกับผู้ควบคุมข้อมูลหรือกฎหมายใดๆ

7.4 กำหนดขั้นตอนและวิธีในการทำลายข้อมูล และเก็บรักษาคำอธิบายชุดข้อมูล (Metadata) ของข้อมูลที่ทำลายไว้เพื่อใช้สำหรับการตรวจสอบในภายหลัง

7.5 สร้างความรู้และความเข้าใจในการจัดเก็บและทำลายข้อมูลแก่ผู้ที่เกี่ยวข้อง

ส่วนที่ 6
สิทธิการเข้าถึงข้อมูล

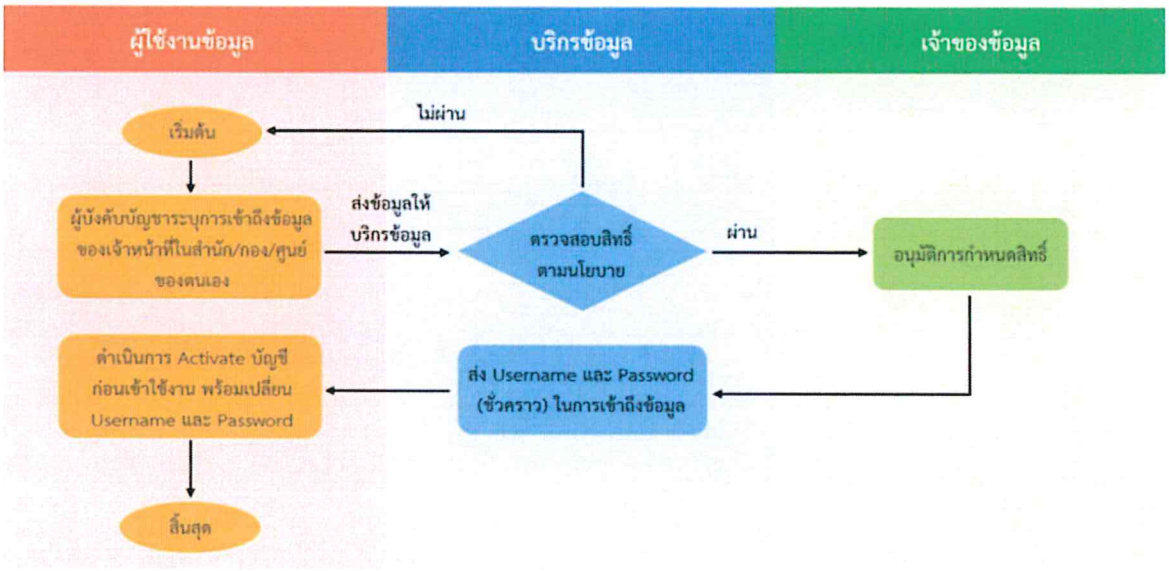
วัตถุประสงค์

เพื่อกำหนดมาตรฐาน กระบวนการ บุคลากร หน้าที่และความรับผิดชอบ และเทคโนโลยีที่ พพ. ต้องปฏิบัติในการกำหนดสิทธิการเข้าถึงข้อมูล

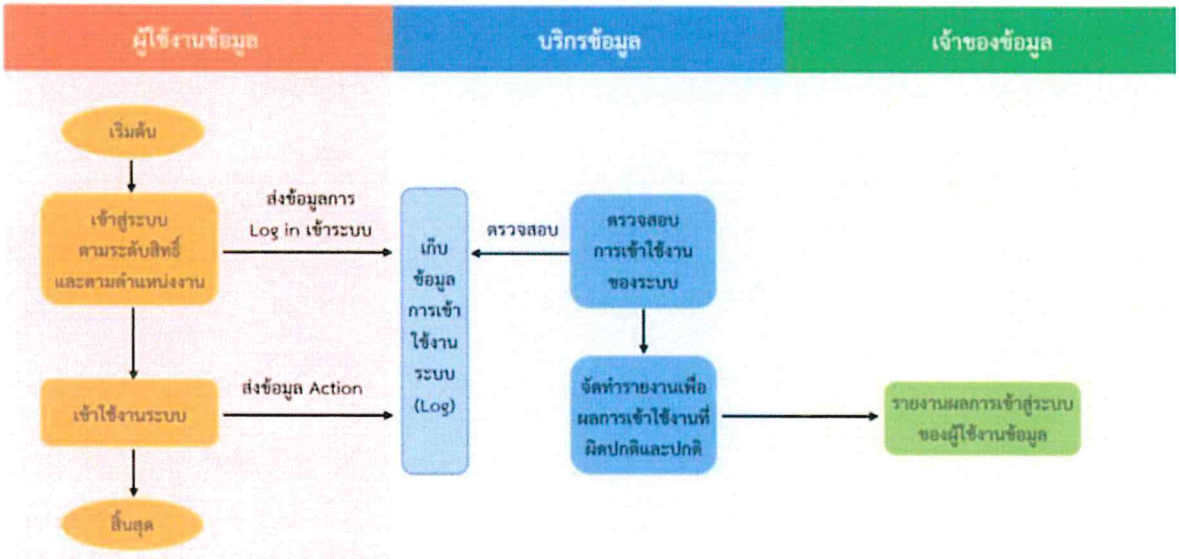
แนวปฏิบัติ

1. ทุกชุดข้อมูลต้องระบุสิทธิในการเข้าถึงข้อมูลเป็นเมทริกซ์ CRUD (Create – Read – Update – Delete) ในการระบุสิทธิการสร้าง เข้าถึงเพื่ออ่าน เข้าถึงเพื่อแก้ไข และหรือลบข้อมูล
2. สิทธิในการเข้าถึงข้อมูล กำหนดโดยตำแหน่งงาน และสิทธิในการเข้าระบบ กำหนดเป็นรายบุคคล
3. ทุกแอพพลิเคชั่นหรือระบบ ต้องปฏิบัติตามสิทธิการเข้าถึงข้อมูล
4. บริกรข้อมูล (สารสนเทศ) ทำการตรวจสอบการเข้าถึงข้อมูลในประเด็นการเข้าถึงที่ผิดนโยบาย หรือการเข้าถึงที่ผิดปกติที่มีความเสี่ยงต่อการโดนโจมตี และต้องรายงานต่อคณะกรรมการธรรมาภิบาลข้อมูล
5. ผู้ใช้งานข้อมูล ซึ่งนำเข้าข้อมูลปฏิบัติตามสิทธิการเข้าถึงข้อมูลที่คณะกรรมการธรรมาภิบาลข้อมูลกำหนด
6. บริกรข้อมูลทุกส่วนงานต้องทำการระบุสิทธิเข้าถึงของข้อมูลตามตำแหน่งงาน ให้เป็นไปตามมาตรฐาน โดยกำกับดูแลความถูกต้องและตรวจสอบโดยฝ่ายสารสนเทศ
7. มีการทบทวนสิทธิการเข้าถึงข้อมูล อย่างน้อยปีละ 1 ครั้ง
8. การสร้างและการเข้าถึงข้อมูลในทุกกิจกรรมต้องมีการเก็บบันทึก

กระบวนการขอสิทธิการเข้าถึงข้อมูลและกระบวนการตรวจสอบสิทธิการเข้าถึงข้อมูล ดังแสดงในรูปที่ 6 และรูปที่ 7 ตามลำดับ



รูปที่ 6 กระบวนการขอสิทธิ์การเข้าถึงข้อมูล



รูปที่ 7 กระบวนการตรวจสอบสิทธิการเข้าถึงข้อมูล

ส่วนที่ 7
คุณภาพข้อมูล

วัตถุประสงค์

เพื่อกำหนดมาตรฐาน กระบวนการ บุคลากร หน้าที่และความรับผิดชอบ และเทคโนโลยีที่ พพ. ต้องปฏิบัติในการดำเนินงานด้านคุณภาพข้อมูล (Data Quality)

แนวปฏิบัติ

1. ชุดข้อมูลทุกชุดต้องมีคุณภาพข้อมูลอย่างน้อยครอบคลุมถึงความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความสอดคล้องกัน (Consistency) และความเป็นปัจจุบัน (Timeliness)

1.1 ความถูกต้องของข้อมูลต้องมีการตรวจสอบโดยบริกรข้อมูล และแก้ไขโดยเจ้าของข้อมูล

1.2 ความครบถ้วนของข้อมูลสามารถตรวจสอบได้

1.3 ความต้องกันของข้อมูลสามารถตรวจสอบได้กับมาตรฐานข้อมูลที่ตั้งไว้ในแต่ละชุดข้อมูล

1.4 ความเป็นปัจจุบันต้องมีการเปรียบเทียบกับฟิลด์อ้างอิงที่เป็นเกณฑ์เวลาตามมาตรฐาน

2. คุณภาพข้อมูลต้องดำเนินการโดยเจ้าของข้อมูล ผู้ใช้ข้อมูล และบริกรข้อมูลในสำนัก/กอง/ศูนย์/กลุ่มงาน และเห็นชอบโดยคณะกรรมการธรรมาภิบาลข้อมูล

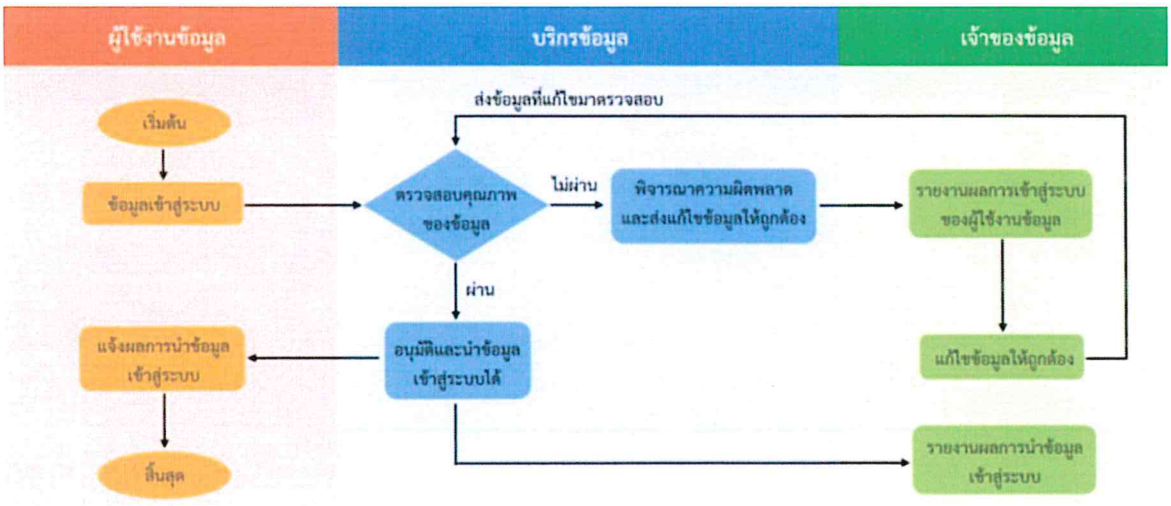
3. คุณภาพข้อมูลจะต้องแนบไปกับการใช้ข้อมูลและคำอธิบายชุดข้อมูล (Metadata)

4. คุณภาพข้อมูลต้องมีการทบทวนอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

5. เมื่อมีการนำเข้าข้อมูล ผู้ใช้ข้อมูลมีหน้าที่ตรวจสอบคุณภาพข้อมูลก่อนนำเข้า

6. เมื่อข้อมูลถูกนำเข้าไปแล้วบริกรข้อมูลแต่ละสำนัก/กอง/ศูนย์/กลุ่มงาน จะทำการตรวจสอบคุณภาพข้อมูลโดยรวมอีกครั้ง ถ้ามีความผิดพลาด บริกรข้อมูลจะต้องแจ้งไปยังเจ้าของข้อมูลให้รับทราบ และแจ้งให้เจ้าของข้อมูลนำเข้าข้อมูลดำเนินการแก้ไข

7. ถ้ามีความจำเป็นต้องทบทวนนโยบาย ให้นำเรื่องเข้าสู่การประชุมของคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) กระบวนการตรวจสอบคุณภาพข้อมูลดังแสดงในรูปที่ 8



รูปที่ 8 กระบวนการตรวจสอบคุณภาพข้อมูล

ส่วนที่ 8
การปฏิบัติงานตามหลักธรรมาภิบาลข้อมูล

วัตถุประสงค์

เพื่อระบุบทบาทหน้าที่ของบุคลากรที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล

การปฏิบัติหน้าที่

1. คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของ พพ. มีหน้าที่รับผิดชอบ ดังนี้

1.1 กำหนดความต้องการ ให้ข้อเสนอแนะ และอนุมัติ นโยบาย ข้อมูล คุณภาพ ความมั่นคงปลอดภัย ชั้นความลับ ระเบียบ และข้อบังคับอื่นๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการจัดลำดับความสำคัญของข้อมูลในการดำเนินการธรรมาภิบาลข้อมูล

1.2 ให้ความเห็นและข้อเสนอแนะในด้านการจัดการและการกำกับดูแลข้อมูลต่อบริกรข้อมูล มีส่วนร่วมในการให้การสนับสนุนและพิจารณานโยบายด้านข้อมูล และให้การสนับสนุนทรัพยากรจากแต่ละกอง/ศูนย์/กลุ่มงาน เพื่อการดำเนินงานตามนโยบายและแนวทางปฏิบัติธรรมาภิบาลข้อมูล

1.3 นำข้อมูลและวิเคราะห์ข้อมูล เพื่อจัดทำยุทธศาสตร์และดำเนินการกำกับดูแลข้อมูลให้มีคุณภาพ นำแนวปฏิบัติและมาตรฐานของหน่วยงานไปปรับปรุง รวมถึงทบทวนและติดตามการดำเนินงานธรรมาภิบาลข้อมูล

1.4 เป็นตัวกลางระหว่างหน่วยงานภาครัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้ข้อมูลของหน่วยงานมีคุณภาพและเกิดประโยชน์สูงสุดต่อหน่วยงาน

1.5 เผยแพร่ข้อสรุป มาตรฐาน หรือนโยบายที่มีการอนุมัติจากที่ประชุมคณะกรรมการธรรมาภิบาลข้อมูลให้บุคลากร พพ. ได้รับทราบ

2. บริกรข้อมูล มีหน้าที่รับผิดชอบ คือ

2.1 ดำเนินการกำกับดูแล ติดตาม และรายงานผลการดำเนินการธรรมาภิบาลข้อมูล

2.2 นิยามข้อมูล นิยามความต้องการด้านคุณภาพ และความมั่นคงปลอดภัยร่วมกับเจ้าของข้อมูล

2.3 บริหารจัดการ ควบคุมการดำเนินงานตามนโยบายจากคณะกรรมการธรรมาภิบาลข้อมูล ติดตามการดำเนินงานและข้อเสนอแนะเพื่อเป็นข้อมูลให้แก่ผู้บริหารระดับสูงด้านข้อมูลหรือคณะกรรมการธรรมาภิบาลข้อมูล

2.4 ตรวจสอบความสอดคล้องกันระหว่างนโยบายกับการดำเนินการต่อข้อมูลตรวจสอบ คุณภาพข้อมูล วิเคราะห์ผลจากการตรวจสอบและรายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้องอื่นๆ

2.5 ประสานงานในปัญหาด้านข้อมูลจากบุคลากรในส่วนงานเดียวกัน

3. เจ้าของข้อมูล มีหน้าที่

3.1 ตรวจสอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบหรือกฎหมาย

3.2 ทบทวนและร่วมอนุมัติการดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูล

3.3 ดำเนินงานตรวจสอบคุณภาพข้อมูลและการเชื่อมโยงข้อมูลร่วมกับบริกรข้อมูล

3.4 ระบุสิทธิในการเข้าถึงข้อมูล และจัดชั้นความลับของข้อมูล เพื่อให้คณะกรรมการธรรมาภิบาลข้อมูลอนุมัติ

3.5 เป็นผู้ควบคุมการดำเนินงานของผู้ใช้ข้อมูล

4. ผู้สร้างข้อมูล มีหน้าที่

4.1 บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้

4.2 ทำงานร่วมกับบริกรข้อมูลเพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูล และความมั่นคงปลอดภัยของข้อมูล

ส่วนที่ 9
กฎ ระเบียบที่เกี่ยวข้อง

วัตถุประสงค์

เพื่ออ้างอิงกฎหมาย ระเบียบ ข้อบังคับ แนวนโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ

แนวปฏิบัติ

1. <u>การเปิดเผยข้อมูล</u>

การเปิดเผยข้อมูลเป็นสิ่งจำเป็นต่อการดำเนินงานของหน่วยงานภาครัฐ เพื่อแสดงถึงความโปร่งใสในการดำเนินงาน และความสามารถในการตรวจสอบได้จากผู้ที่มีส่วนได้ส่วนเสียทุกภาคส่วน รวมถึงเป็นการสนับสนุนให้มีการนำข้อมูลที่เปิดเผยไปสร้างนวัตกรรมผลิตภัณฑ์และบริการเพื่อยกระดับการพัฒนาประเทศ ทั้งนี้ กฎหมายที่เกี่ยวข้องกับการเปิดเผยข้อมูลมีดังนี้

1.1 รัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2560 ในมาตราที่ 59 ได้ระบุว่า รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการ

1.2 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ให้มีการเปิดเผยข้อมูลหรือข่าวสารสาธารณะที่หน่วยงานของรัฐจัดทำและครอบครองในรูปแบบและช่องทางดิจิทัล เพื่อให้ประชาชนเข้าถึงโดยสะดวกมีส่วนร่วมและตรวจสอบการดำเนินงานของรัฐ และสามารถนำข้อมูลไปพัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่างๆ

1.3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มี 3 ประเด็นที่เกี่ยวกับการเปิดเผยข้อมูล ได้แก่

1) ข้อมูลภาครัฐต้อง “เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น”
2) กำหนดหลักเกณฑ์และกลไกการเปิดเผยข้อมูล
3) กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้

2. <u>การเชื่อมโยงและแลกเปลี่ยนข้อมูล</u>

การเชื่อมโยงและแลกเปลี่ยนข้อมูลเป็นสิ่งสำคัญต่อการบูรณาการการดำเนินงานระหว่างหน่วยงานภาครัฐและเป็นประโยชน์ในการขอใช้บริการจากประชาชนหรือหรือหน่วยงานที่เกี่ยวข้อง โดยกฎหมายที่เกี่ยวข้อง คือ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ที่กำหนดให้มีการพัฒนามาตรฐาน หลักเกณฑ์ และวิธีการเกี่ยวกับดิจิทัล และพัฒนาโครงสร้างพื้นฐานด้านดิจิทัลที่จำเป็นให้เป็นไปตามมาตรฐานสากล เพื่อสร้างและพัฒนากระบวนการทำงานของหน่วยงานของรัฐให้มีความสอดคล้องและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกัน รวมทั้งมีความมั่นคงปลอดภัยและน่าเชื่อถือ โดยมีการบูรณาการและสามารถทำงานร่วมกันอย่างเป็นเอกภาพ เกิดการพัฒนาการบริการภาครัฐที่มีประสิทธิภาพและนำไปสู่การบริหารราชการและการบริการประชาชนแบบบูรณาการเพื่อให้เข้าถึงบริการได้อย่างสะดวก

3. <u>การคุ้มครองข้อมูลส่วนบุคคล</u>

การคุ้มครองข้อมูลส่วนบุคคล (Privacy Data Protection) เป็นสิ่งสำคัญที่ภาครัฐต้องดำเนินการ โดยจะต้องมีการรวบรวม จัดเก็บ ใช้หรือเผยแพร่ข้อมูลส่วนบุคคลของผู้ใช้บริการในรูปแบบของข้อมูลอิเล็กทรอนิกส์เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล และสร้างความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์ของประชาชนโดยมีกฎหมายที่เกี่ยวข้อง ดังนี้

3.1 พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้ ซึ่งจะต้องมีการพิจารณาในกรณีที่เป็นข้อมูลส่วนบุคคลที่ต้องได้รับการคุ้มครองอย่างมีหลักเกณฑ์

3.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการกำหนดหลักเกณฑ์ กลไกและมาตรการที่กำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

3.3 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 ได้ระบุเรื่องการคุ้มครองข้อมูลส่วนบุคคลไว้ว่า “กำหนดให้ภาครัฐที่ให้บริการทางอิเล็กทรอนิกส์ต้องมีนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล”

4. <u>การรักษาความลับ</u>

การรักษาความลับทางราชการเป็นสิ่งจำเป็นต่อการดำเนินงานของหน่วยงาน เพื่อเป็นการป้องกันความเสียหายที่จะเกิดขึ้นต่อภาครัฐ ทั้งในด้านชื่อเสียง การเงิน ความสามารถในการพัฒนาประเทศและความมั่นคงของประเทศ โดยมีกฎหมายและระเบียบที่เกี่ยวข้อง ดังนี้

4.1 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ได้มีข้อกำหนดที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ ได้แก่ กำหนดนิยามข้อมูลข่าวสารลับและกำหนดหลักเกณฑ์และวิธีการในการรักษาความลับของหน่วยงานภาครัฐ

4.2 แนวทางปฏิบัติในการรักษาความปลอดภัยเกี่ยวกับบุคคล เอกสาร และสถานที่ที่จัดทำขึ้นจากระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552

5. <u>ประเด็นอื่นๆ ที่เกี่ยวข้องกับเรื่องธรรมาภิบาลข้อมูลภาครัฐ</u>

5.1 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 กำหนดให้หน่วยงานรัฐจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล โดยมีการบริหารจัดการและบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล โดยมุ่งหมายในการเพิ่มประสิทธิภาพและอำนวยความสะดวกในการให้บริการและเข้าถึงประชาชน และในการเปิดเผยข้อมูลภาครัฐต่อสาธารณะและสร้างการมีส่วนร่วมของทุกภาคส่วน

5.2 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมและกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องดำเนินการตามมาตรฐานด้านการรักษาความปลอดภัยไซเบอร์ เพื่อรักษาสถานะของข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์

5.3 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 โดยกำหนดให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยการเข้าถึงข้อมูลสารสนเทศในระดับเคร่งครัด ระดับกลางหรือระดับพื้นฐาน ให้หน่วยงานหรือองค์กรหรือส่วนงานของหน่วยงานหรือองค์กรปฏิบัติตามมาตรฐาน

ส่วนที่ 10
กระบวนการดำเนินงานด้านธรรมาภิบาลข้อมูลของ พพ.

กระบวนการดำเนินงานด้านธรรมาภิบาลข้อมูลของ พพ.

การบริหารจัดการข้อมูลเป็นสิ่งสำคัญสำหรับทุกหน่วยงาน ซึ่งแต่ละหน่วยงานต้องตระหนักว่าข้อมูลที่มีอยู่เป็นทรัพย์สินที่มีค่าและจากการเกิดขึ้นของข้อมูลที่มีปริมาณมหาศาล ไม่ว่าจะเป็นข้อมูลที่รวบรวมมาโดยอัตโนมัติจากระบบหรืออุปกรณ์ต่าง ๆ หรือข้อมูลที่เกิดขึ้นจากการป้อนข้อมูลหรือโต้ตอบกับผู้ใช้งาน เพื่อให้หน่วยงานสามารถนำข้อมูลเหล่านี้ไปประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ จึงต้องได้รับการบริหารจัดการอย่างถูกต้องเหมาะสม และสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของหน่วยงาน ธรรมาภิบาลข้อมูลภาครัฐจึงถูกจัดทำขึ้นเพื่อกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูล ดังนั้น กระบวนการดำเนินการด้านธรรมาภิบาลข้อมูลของ พพ. จึงเป็นขั้นตอนที่ใช้สำหรับการกำกับดูแลการดำเนินการใด ๆ ต่อข้อมูลให้เป็นไปตามกฎระเบียบ ข้อบังคับ หรือนโยบายที่เกี่ยวข้องกับข้อมูล กระบวนการธรรมาภิบาลข้อมูลภาครัฐ เริ่มตั้งแต่การวางแผนไปจนถึงการปรับปรุงอย่างต่อเนื่องดังนี้

1. การวางแผน (Plan) คือ การวางแผนเริ่มตั้งแต่กำหนดวิสัยทัศน์และประเด็นปัญหา ซึ่งเป็นส่วนที่สำคัญเนื่องจากเป็นจุดเริ่มต้นที่จะกำหนด กฎระเบียบ นโยบาย มาตรฐาน หรือแนวทางปฏิบัติต่างๆ เพื่อใช้ในการกำกับดูแลและการบริหารจัดการข้อมูลของหน่วยงาน

2. การปฏิบัติ (Do) คือ การดำเนินงานของคณะกรรมการการบริหารจัดการข้อมูลที่เกี่ยวข้องโดยมีรายละเอียดและแนวปฏิบัติที่ได้กำหนดไว้

3. การตรวจสอบ วัดผล และรายงาน (Check, Measure and Report) คือ การตรวจสอบบริกรข้อมูลจะดำเนินการตรวจสอบความสอดคล้องกันระหว่าง กฎระเบียบ นโยบาย และมาตรฐานที่กำหนด กับการปฏิบัติงานของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ โดยทำการวัดผลด้านคุณภาพข้อมูลซึ่งมีรายละเอียดและแนวทางการวัดผล

4. การปรับปรุงอย่างต่อเนื่อง (Continual Improvement) คือ การจัดให้มีการดำเนินงาน ติดตามรายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูลรายงาน คุณภาพข้อมูล รายงานความมั่นคงปลอดภัย รายงานความเสี่ยงต่อข้อมูล จะถูกใช้สำหรับการปรับปรุงกระบวนการธรรมาภิบาลข้อมูลภาครัฐ นโยบาย กฎ ระเบียบข้อบังคับที่เกี่ยวข้องกับข้อมูล เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ เกณฑ์การวัดระดับคุณภาพข้อมูล และโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ