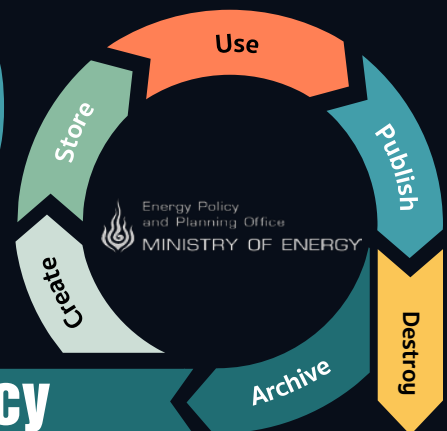


นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

EPPP

Data Governance Policy



สำนักงานนโยบายและแผนพลังงาน

พฤษภาคม 2566

นโยบายธรรมาภิบาลข้อมูล
(Data Governance Policy)



สำนักงานนโยบายและแผนพลังงาน

พฤษภาคม 2566

นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy)

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีการบริการงานภาครัฐ และการจัดทำบริการสาธารณะให้เป็นไปด้วยความสะดวกรวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน รวมทั้งกำหนดให้มีการบริหารจัดการและบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องและเชื่อมโยงเข้าด้วยกันอย่างมั่นคง ปลอดภัย และมีธรรมาภิบาล ประกอบกับคณะกรรมการพัฒนารัฐบาลดิจิทัล ได้ออกประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องธรรมาภิบาลข้อมูลภาครัฐ เมื่อวันที่ 12 มีนาคม 2563 กำหนดให้หน่วยงานมีธรรมาภิบาลข้อมูลภาครัฐเพื่อเป็นหลักการและแนวทางในการดำเนินงานในการกำกับดูแลข้อมูลภาครัฐในระดับหน่วยงานให้สอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้ข้อมูลมีการจัดเก็บอย่างเป็นระบบ มีคุณภาพ ถูกต้อง ครบถ้วน สนับสนุนการให้บริการแก่ประชาชนอย่างสะดวกรวดเร็วและมีประสิทธิภาพ

ดังนั้น เพื่อให้การบริหารจัดการข้อมูลของสำนักงานนโยบายและแผนพลังงาน (สนพ.) เป็นไปอย่างเหมาะสม มีประสิทธิภาพ ข้อมูลมีคุณภาพ ถูกต้อง ครบถ้วน มั่นคงปลอดภัย และสามารถดำเนินการได้อย่างต่อเนื่อง รวมทั้งการป้องกันภัยคุกคามหรือปัญหาที่อาจเกิดขึ้นจากการบริหารจัดการและการใช้ข้อมูล ตลอดจนให้เกิดความสอดคล้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐ จึงเห็นสมควรกำหนดนโยบายธรรมาภิบาลข้อมูล โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนการปฏิบัติงาน (Procedure) และวิธีการปฏิบัติ (Work Instruction) ให้ครอบคลุมในด้านต่างๆ ของธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล โดยมีขอบเขตและวัตถุประสงค์ ดังนี้

ขอบเขต

1. การจัดทำนโยบายการดำเนินการด้านธรรมาภิบาลข้อมูลมีขอบเขตครอบคลุมการบริหารจัดการข้อมูลให้เป็นอย่างเหมาะสม มีประสิทธิภาพ มีคุณภาพ มีความมั่นคงปลอดภัย มีการเชื่อมโยง และสามารถดำเนินงานได้อย่างต่อเนื่องและยั่งยืน
2. นโยบายข้อมูลนี้ บังคับใช้กับผู้ดูแลข้อมูล ผู้ใช้ข้อมูล และเจ้าหน้าที่ที่เกี่ยวข้องของกับข้อมูลของ สนพ. โดยต้องเผยแพร่ให้บุคลากรทุกระดับใน สนพ. ได้รับทราบ และต้องถือปฏิบัติอย่างเคร่งครัด
3. ต้องมีการดำเนินการตรวจสอบและประเมินผลการปฏิบัติเพื่อปรับปรุงนโยบายตามความเหมาะสม

วัตถุประสงค์

1. เพื่อให้ สนพ. มีนโยบายข้อมูล (Data Policy) ที่สนับสนุนการดำเนินการบริหารจัดการข้อมูลภายใต้กรอบธรรมาภิบาลข้อมูลภาครัฐและระเบียบปฏิบัติที่ถูกต้อง
2. เพื่อกำหนดขอบเขตของระบบบริหารและการจัดการข้อมูลของ สนพ. โดยอ้างอิงตามกรอบธรรมาภิบาลข้อมูลภาครัฐและมีการปรับปรุงอย่างสม่ำเสมอ
3. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้แก่ผู้บริหาร บุคลากร และผู้ที่เกี่ยวข้องให้มีความตระหนักถึงความสำคัญของธรรมาภิบาลข้อมูล การบริหารจัดการข้อมูล และปฏิบัติตามอย่างเคร่งครัด
4. เพื่อใช้เป็นหลักในการพัฒนาและปรับปรุงธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล ให้ข้อมูลมีคุณภาพ และมีความมั่นคงปลอดภัยตามหลักมาตรฐานสากลตามนโยบายการดำเนินงานด้านธรรมาภิบาลข้อมูล

คำนิยาม

“**สนพ.**” หมายความว่า สำนักงานนโยบายและแผนพลังงาน

“**ผู้บังคับบัญชา**” หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ สนพ.

“**คณะกรรมการธรรมาภิบาลข้อมูล**” (Data Governance Council) หมายความว่า คณะกรรมการธรรมาภิบาลข้อมูลของ สนพ.

“**ผู้บริหารระดับสูงด้านข้อมูล (Chief Data Officer: CDO)**” หมายความว่า ผู้บริหารระดับสูงที่รับผิดชอบด้านการกำกับดูแลข้อมูลของ สนพ.

“**บุคลากร**” หมายความว่า ผู้บริหาร ข้าราชการ พนักงานราชการและลูกจ้างของ สนพ.

“**หน่วยงานภายนอก**” หมายความว่า องค์กรหรือหน่วยงานที่ สนพ. อนุญาตให้มีสิทธิในการเข้าถึงหรือใช้ข้อมูล หรือใช้งานระบบสารสนเทศของ สนพ. โดยจะได้รับสิทธิตามประเภทการใช้งาน และต้องรับผิดชอบในการไม่เปิดเผยความลับของ สนพ. โดยไม่ได้รับอนุญาต

“**ระบบคอมพิวเตอร์**” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่งชุดหรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“**ระบบสารสนเทศ**” หมายความว่า ซอฟต์แวร์ระบบหรือซอฟต์แวร์ประยุกต์ที่ใช้ในการปฏิบัติงานของ สนพ.

“**ข้อมูล (Data)**” หมายความว่า สิ่งสื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าจะการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั่นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง ภาพวาด ภาพถ่าย ภาพฉายดาวเทียม ภาพยนตร์ การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่ยังไม่ปรากฏได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

“**ชุดข้อมูล (Datasets)**” หมายความว่า การนำข้อมูลจากหลายแหล่งมารวบรวมเพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล

“**บัญชีข้อมูล (Data Catalog)**” หมายความว่า เอกสารแสดงรายการของชุดข้อมูลที่จำแนกแยกแยะ โดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของ สนพ.

“**พจนานุกรมข้อมูล (Data Dictionary)**” หมายความว่า ตารางหรือข้อมูลที่ใช้อธิบายรายละเอียดของข้อมูลในแต่ละแถวหรือคอลัมน์

“**เมทาดาตา (Metadata)**” หมายความว่า คำอธิบายชุดข้อมูลดิจิทัลเพื่อให้ทราบรายละเอียดเกี่ยวกับโครงสร้างของข้อมูล เนื้อหาสาระ รูปแบบการจัดเก็บ แหล่งข้อมูล และสิทธิในการเข้าถึงข้อมูล

“**การบริหารจัดการข้อมูล (Data Management)**” หมายความว่า ขั้นตอนการสร้าง การรวบรวม การจัดเก็บ การจัดเก็บถาวร การทำลาย การประมวลผล การใช้ การแลกเปลี่ยน การเชื่อมโยง และการเปิดเผยข้อมูล

“**บริการข้อมูล (Data Steward)**” หมายความว่า บุคลากรของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารและจากสำนัก/กอง ที่ได้รับมอบหมายให้มีหน้าที่ดำเนินงานธรรมาภิบาลข้อมูล

“**ผู้สร้างข้อมูล (Data Creator)**” หมายความว่า บุคลากรของกอง/ศูนย์/กลุ่มงาน ที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ รวมทั้งมีหน้าที่ในการทำงานร่วมกับบริการข้อมูล เพื่อ ตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัยของข้อมูล

“**ผู้ใช้ข้อมูล (Data User)**” หมายความว่า บุคคลที่ได้รับอนุญาต (Authorized Users) ให้สามารถเข้ามาใช้งาน บริหาร หรือดูแลรักษาระบบสารสนเทศของ สนพ. ตามสิทธิ์และหน้าที่ความรับผิดชอบ

“**ผู้ดูแลระบบสารสนเทศ (System Administrator)**” หมายความว่า บุคลากรของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบ และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

“**บุคคลภายนอก**” หมายความว่า ผู้ประกอบการหรือผู้ให้บริการภายนอก (Third Party) ผู้ร้องเรียนเรื่องราวต่างๆ ที่เกี่ยวข้องกับการทำงานของ สนพ. โดยบุคคลภายนอกจะใช้ระบบสารสนเทศที่ สนพ. เตรียมไว้ให้บริการสำหรับบุคคลภายนอก

“**เจ้าของข้อมูล (Data Owner)**” หมายความว่า บุคลากรหน่วยงานที่มีหน้าที่รับผิดชอบข้อมูล ของ สนพ. ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยเจ้าของข้อมูลเป็นผู้ที่รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรง หากข้อมูลเหล่านั้นเกิดสูญหาย

“**สิทธิของผู้ใช้งาน**” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของ สนพ. โดย สนพ. จะเป็นผู้พิจารณาสิทธิในการใช้ทรัพย์สิน

“**บัญชีผู้ใช้งาน (User Account)**” หมายความว่า รายชื่อผู้มีสิทธิใช้งาน (User Name) และ รหัสผ่าน (Password) เพื่อการเข้าสู่ระบบคอมพิวเตอร์และระบบเครือข่ายหรือระบบสารสนเทศ

“**คุณภาพข้อมูล (Data Quality)**” หมายความว่า ตัวชี้วัดเชิงปริมาณ (Quantitative Measurement) ของความพร้อมใช้ข้อมูลอย่างมีประโยชน์ โดยมี 4 องค์ประกอบ ได้แก่ ความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องกัน (Consistency) และความเป็นปัจจุบัน (Timeliness)

“**สารสนเทศ (Information)**” หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งาน สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

“**การเข้าถึง**” หมายความว่า การเข้าสถานที่ การใช้งานทางอิเล็กทรอนิกส์ หรือกายภาพ รวมถึง การรับรู้ซึ่งข้อมูล

“**การควบคุมการเข้าถึง**” หมายความว่า การอนุญาต การกำหนดสิทธิและการเปลี่ยนแปลง การเพิกถอน หรือการยกเลิกสิทธิการเข้าถึง

“การควบคุมการใช้งานสารสนเทศ” หมายความว่า การตรวจสอบ การอนุมัติ และการกำหนด สิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ การเพิกถอนหรือการยกเลิกสิทธิการเข้าถึง

“ทรัพย์สิน (Asset)” หมายความว่า สิ่งที่มีคุณค่าหรือมูลค่าต่อหน่วยงานและเป็นทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศที่หน่วยงานเป็นเจ้าของ เช่า ว่าจ้าง พัฒนา หรือจัดซื้อ โดยแบ่งแยก ออกเป็นประเภทต่างๆ ได้ดังนี้ สารสนเทศ (Information) ซอฟต์แวร์ (Software) ทรัพย์สินที่มีรูปร่าง (Physical Asset) บริการสาธารณูปโภคพื้นฐาน (Service) และบุคลากร (People)

ส่วนที่ 1 บทนำ

ข้อมูล

จัดเป็นทรัพย์สินที่สำคัญในการดำเนินงานของหน่วยงานภาครัฐ สำนักงานนโยบายและแผนพลังงาน (สนพ.) ตระหนักถึงความสำคัญของการนำข้อมูลมาใช้สนับสนุนการขับเคลื่อนนโยบายเศรษฐกิจและสังคมดิจิทัล และเพื่อให้การได้มาซึ่งข้อมูลและการนำไปใช้เป็นไปอย่างถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย รักษาความเป็นส่วนตัว และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพ เพื่อให้ข้อมูลมีคุณภาพ และมีการเชื่อมโยงภายใต้กรอบธรรมาภิบาลข้อมูลโดยมีคณะกรรมการธรรมาภิบาลข้อมูลทำหน้าที่กำหนดยุทธศาสตร์ และเป้าหมาย กำหนดขอบเขตและตรวจสอบสภาพแวดล้อมธรรมาภิบาลข้อมูล รวมทั้งกำหนดนิยามและมาตรฐานของข้อมูล ดังแสดงในภาพที่ 1



ภาพที่ 1 กรอบธรรมาภิบาลข้อมูลของ สนพ

วิสัยทัศน์ธรรมาภิบาลข้อมูล

เป็นองค์กรที่มีกรอบธรรมาภิบาลข้อมูล และมีการบริหารจัดการข้อมูลอย่างเหมาะสม

พันธกิจธรรมาภิบาลข้อมูล

1. มีการจัดโครงสร้างองค์กรที่สอดคล้องกับธรรมาภิบาลข้อมูล
2. สร้างข้อมูลที่มีคุณภาพและมีความน่าเชื่อถือในการใช้งานทั้งภายในและภายนอกองค์กร
3. มีกระบวนการบริหารจัดการด้านข้อมูลในองค์กร
4. มีการเสริมสร้างความรู้ความเข้าใจด้านการบริหารจัดการข้อมูลกับบุคลากรทุกระดับ
5. ใช้เทคโนโลยีดิจิทัลมาสนับสนุนการทำงานด้านธรรมาภิบาลข้อมูลอย่างเหมาะสม

เป้าหมายธรรมาภิบาลข้อมูล

1. มีคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) และผู้บริหารระดับสูง ด้านข้อมูล (Chief Data Officer: CDO)
2. มีการกำหนดนโยบายด้านข้อมูลในแต่ละส่วนงานให้ครอบคลุมด้านคุณภาพข้อมูล การเชื่อมโยงข้อมูล และความมั่นคงปลอดภัยข้อมูล
3. บุคลากรมีความรู้ความเข้าใจด้านการจัดการข้อมูลที่ดี เพื่อให้องค์กรไปสู่เป้าหมายร่วมกัน
4. มีความร่วมมือด้านการแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก
5. มีมาตรฐานการดำเนินการข้อมูลเปิด (Open Data)

ยุทธศาสตร์ธรรมาภิบาลข้อมูล

1. กำหนดโครงสร้างธรรมาภิบาลข้อมูล
 - 1.1 จัดตั้งคณะกรรมการธรรมาภิบาลข้อมูลและผู้บริหารระดับสูงด้านข้อมูล
 - 1.2 มีการระบุหน้าที่ความรับผิดชอบของแต่ละส่วนงานด้านข้อมูล
 - 1.3 มีการระบุหน้าที่ความรับผิดชอบของบริการข้อมูล
2. สร้างมาตรฐานธรรมาภิบาลข้อมูล
 - 2.1 มีการกำหนดมาตรฐานในแต่ละส่วนงานให้ครอบคลุมด้านคุณภาพข้อมูล การเชื่อมโยงข้อมูล และความมั่นคงปลอดภัยข้อมูล
 - 2.2 มีการกำหนดกระบวนการ ผู้รับผิดชอบ ข้อตกลงการให้บริการ และตัวชี้วัดในแต่ละส่วนงาน รวมถึงเกณฑ์การประเมินระดับบุคคลให้ครอบคลุมด้านคุณภาพข้อมูล การเชื่อมโยงข้อมูล และความมั่นคงปลอดภัยข้อมูล
 - 2.3 มีการดำเนินการเพื่อรองรับมาตรฐานข้อมูลเปิดภาครัฐในอนาคต
3. พัฒนาบุคลากรด้านธรรมาภิบาลข้อมูล
 - 3.1 มีการสื่อสารองค์กรด้านจัดการข้อมูลที่ดี
 - 3.2 การฝึกอบรมเพื่อเสริมสร้างความรู้และทักษะของบุคลากร

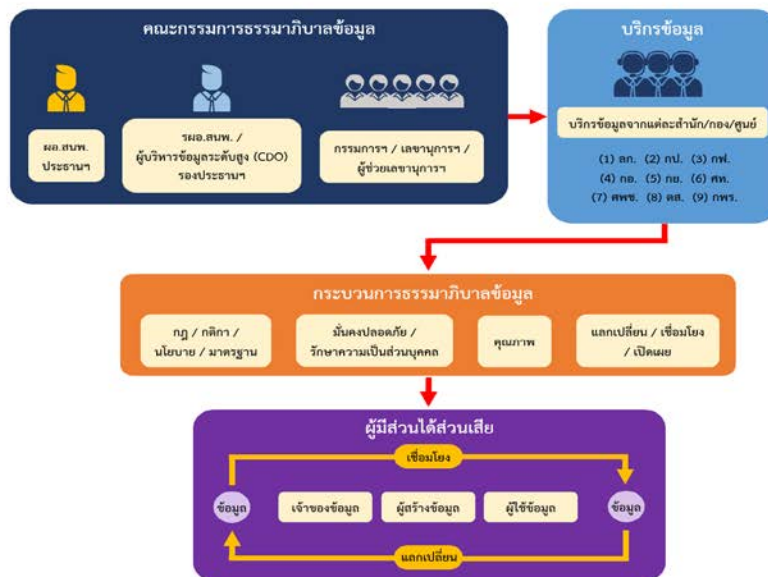
ส่วนที่ 2 โครงสร้างธรรมาภิบาลข้อมูล

วัตถุประสงค์

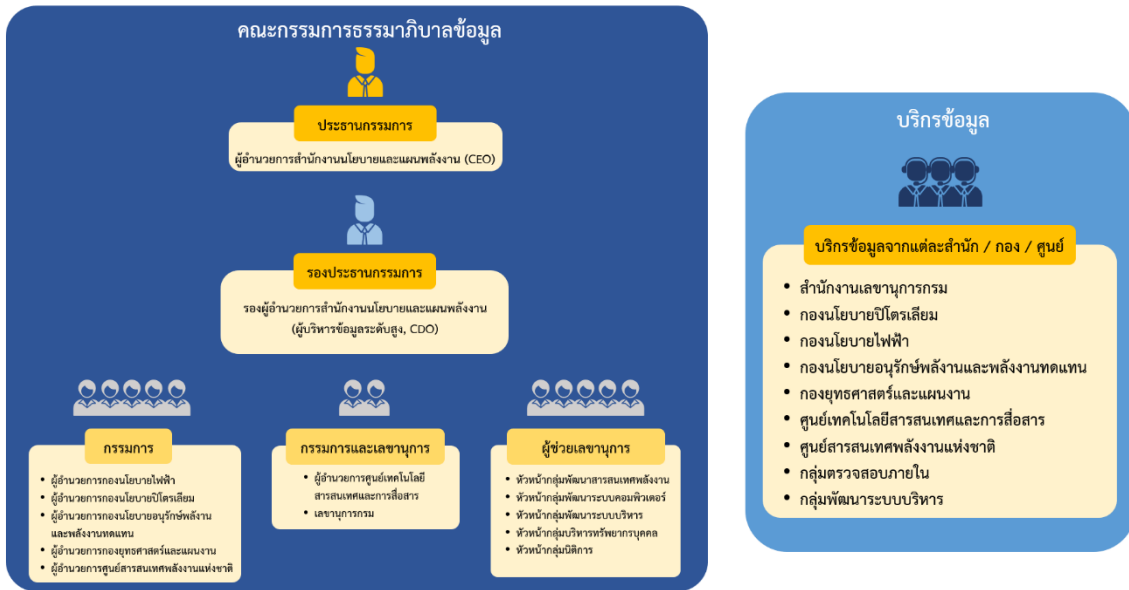
กำหนดโครงสร้างธรรมาภิบาลข้อมูลเพื่อแสดงลำดับชั้นระหว่างกลุ่มบุคคลที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล และแสดงถึงสิทธิในการใช้งานตามลำดับชั้น แนวปฏิบัติ โดยแบ่งออกเป็น 3 ส่วน ประกอบด้วย

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

ดังแสดงในภาพที่ 2 และโครงสร้างตามตำแหน่งดังแสดงในภาพที่ 3



ภาพที่ 2 โครงสร้างธรรมาภิบาลข้อมูลของ สทพ.



ภาพที่ 3 โครงสร้างธรรมาภิบาลข้อมูลตามตำแหน่งของ สนพ.

1. คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)

มีหน้าที่ความรับผิดชอบ ในการกำหนดความต้องการ ให้ข้อเสนอแนะ และอนุมัตินโยบายข้อมูล เกณฑ์การวัดคุณภาพ เกณฑ์ความมั่นคงปลอดภัย ชั้นความลับ ระเบียบ และข้อบังคับอื่นๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการจัดลำดับความสำคัญของข้อมูลในการกำกับดูแลโดยกำหนดให้คณะกรรมการธรรมาภิบาลข้อมูลของ สนพ. ปฏิบัติหน้าที่คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)

2. ทีมบริการข้อมูล (Data Steward Team)

มีหน้าที่ความรับผิดชอบ ในการกำกับดูแล ติดตาม และรายงานผลการดำเนินการธรรมาภิบาลข้อมูล ประกอบด้วย

2.1 บริหารจัดการ ควบคุมการดำเนินงานตามนโยบายจากคณะกรรมการธรรมาภิบาลข้อมูล

2.2 ติดตามการดำเนินงานและข้อเสนอแนะ เพื่อเป็นข้อมูลให้แก่ผู้บริหารระดับสูงด้านข้อมูล หรือ คณะกรรมการธรรมาภิบาลข้อมูล

2.3 ตรวจสอบความสอดคล้องกันระหว่างนโยบายกับการดำเนินการต่อข้อมูล ตรวจสอบ คุณภาพ ข้อมูล วิเคราะห์ผลจากการตรวจสอบ และรายงานผลไปยังคณะกรรมการธรรมาภิบาลข้อมูลและ ผู้ที่เกี่ยวข้องอื่นๆ

2.4 ประสานงานในปัญหาด้านข้อมูลจากบุคลากรในส่วนงานเดียวกัน โดยทั้งหมดนี้จะควบคุมผ่านคณะกรรมการธรรมาภิบาลข้อมูล

3. ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders)

ทำหน้าที่ให้การสนับสนุนธรรมาภิบาลข้อมูลต่อทีมบริการข้อมูลและคณะกรรมการธรรมาภิบาลข้อมูล ประกอบไปด้วย

3.1 เจ้าของข้อมูล (Data Owners) มีหน้าที่ความรับผิดชอบ คือ

- 1) ตรวจสอบดูแลข้อมูลโดยตรง
- 2) สร้างความมั่นใจในการบริหารจัดการข้อมูลให้สอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ

หรือกฎหมาย

- 3) ทบทวนและอนุมัติการดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูล
- 4) ทำความสะอาดข้อมูล (Data Cleansing)
- 5) ให้สิทธิ์ในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

3.2 ผู้สร้างข้อมูล (Data Creator) มีหน้าที่ความรับผิดชอบ คือ

- 1) บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกระบุไว้
- 2) ทำหน้าที่ร่วมกับบริการข้อมูลในการตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและ

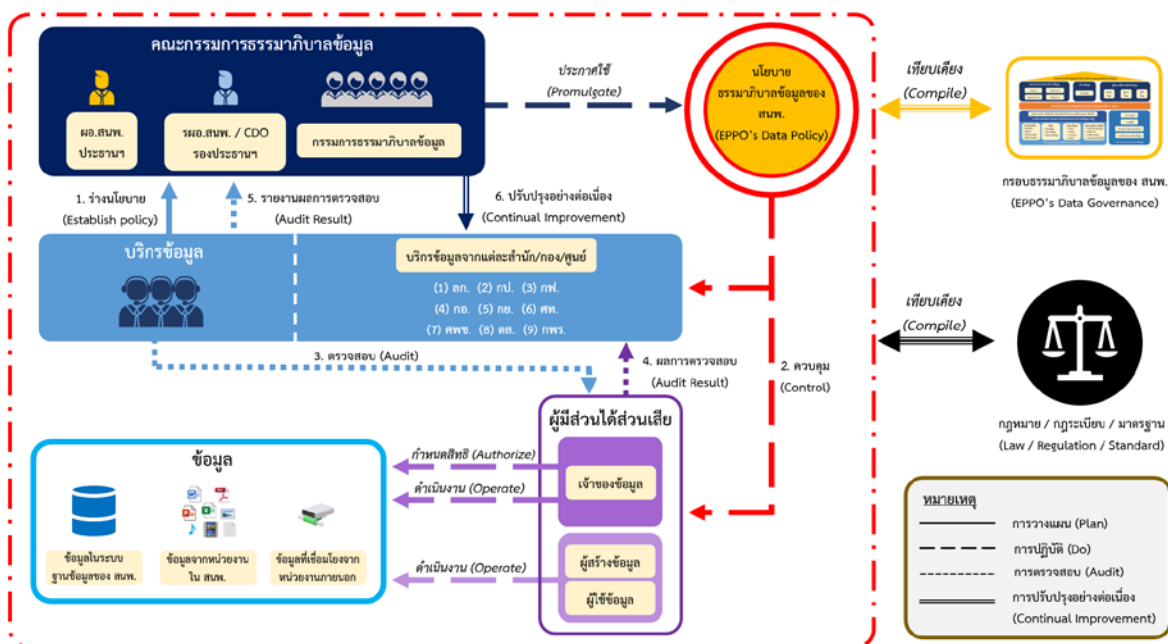
ความมั่นคงปลอดภัย

3.3 ผู้ใช้งานข้อมูล (Data User) มีหน้าที่ความรับผิดชอบ คือ

- 1) นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร
- 2) สนับสนุนการกำกับดูแลข้อมูลโดยการให้ความต้องการในการใช้ข้อมูล
- 3) รายงานประเด็นปัญหาที่พบระหว่างการใช้อข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของ

ข้อมูลไปยังบริการข้อมูล

ขั้นตอนการดำเนินงานภายใต้กรอบธรรมาภิบาลข้อมูลดังแสดงในภาพที่ 4



ภาพที่ 4 ขั้นตอนการดำเนินงานภายใต้กรอบธรรมาภิบาลข้อมูล

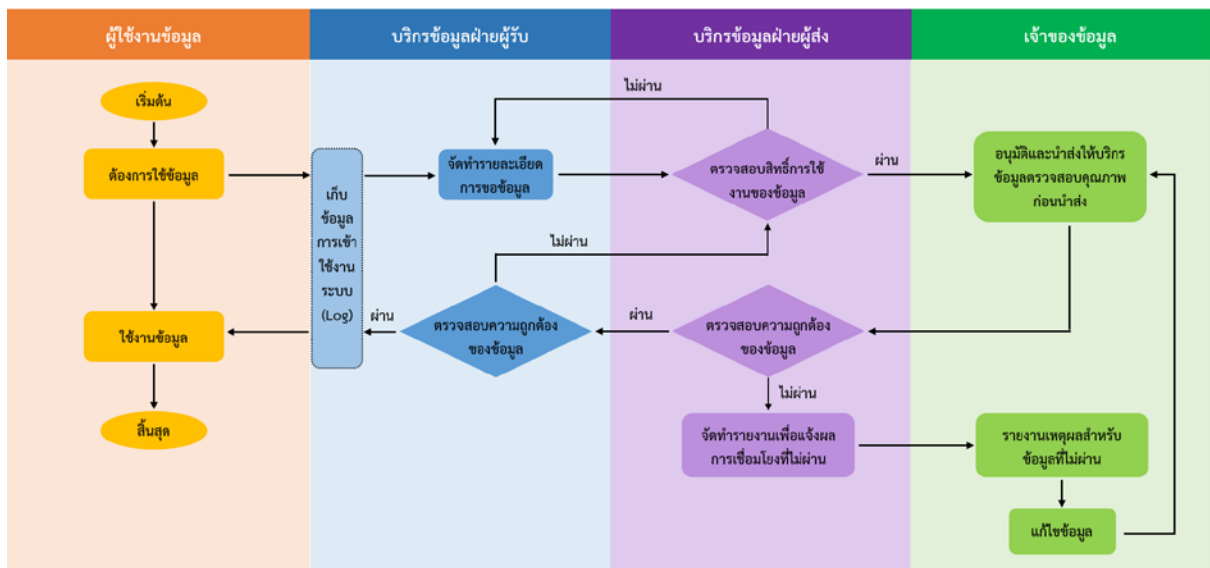
ส่วนที่ 3 การเชื่อมโยงข้อมูล

วัตถุประสงค์

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

แนวปฏิบัติ

1. บริการข้อมูลฝ่ายผู้ส่งจะเป็นผู้รับเรื่อง เมื่อฝ่ายผู้รับพบปัญหาใดๆ เกี่ยวกับการเชื่อมโยงข้อมูล หรือคุณภาพข้อมูลที่ส่งไป บริการข้อมูลของทั้งสองฝ่ายทำหน้าที่ในการตรวจสอบความถูกต้องของข้อมูล
2. บริการข้อมูลฝ่ายผู้ส่งมีหน้าที่ในการรับเรื่องปัญหาที่เกิดขึ้นในการเชื่อมโยงข้อมูล และประสานกับผู้ที่เกี่ยวข้องต่อไป
3. จะต้องมีการจัดทำเอกสารมาตรฐานการเชื่อมโยงข้อมูล ซึ่งประกอบด้วย ชื่อชุดข้อมูล วันและเวลาในการส่งออกข้อมูล และวันและเวลาที่ผู้รับได้รับข้อมูล โดยต้องมีการจัดเก็บบันทึกประวัติการส่ง การรับ และการเชื่อมโยงข้อมูลในแต่ละสำนัก/กอง/ศูนย์/กลุ่มงาน
4. การตรวจสอบข้อมูลจะต้องอ้างอิงตามคำอธิบายชุดข้อมูล (Metadata) และข้อมูลอ้างอิงของชุดข้อมูลนั้น



ภาพที่ 5 กระบวนการเชื่อมโยงระหว่างสำนัก/กอง/ศูนย์/กลุ่มงานของ สนพ.

ส่วนที่ 4

การจัดชั้นความลับของข้อมูล

วัตถุประสงค์

เพื่อกำหนดมาตรฐาน กระบวนการ บุคลากร หน้าที่และความรับผิดชอบ และเทคโนโลยีที่ สนพ. ต้องปฏิบัติในการจัดชั้นความลับของข้อมูล

แนวปฏิบัติ

1. ทุกชุดข้อมูลต้องมีการจัดลำดับชั้นความลับของข้อมูล ดังต่อไปนี้
 - 1.1 ระดับที่ 1 ข้อมูลสาธารณะ ได้แก่ ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ
 - 1.2 ระดับที่ 2 ข้อมูลส่วนบุคคล ได้แก่ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าจะทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
 - 1.3 ระดับที่ 3 ข้อมูลความลับทางราชการ ได้แก่ ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐหรือที่เกี่ยวกับเอกชน ซึ่งมีการกำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือชั้นลับที่สุด
 - 1.4 ระดับที่ 4 ข้อมูลความมั่นคง ได้แก่ ข้อมูลเกี่ยวกับความมั่นคงของรัฐ ที่ส่งผลกระทบต่อความสงบเรียบร้อย เสถียรภาพความเป็นปึกแผ่น ตลอดจนพลผลภัยจากภัยคุกคาม
2. การจัดลำดับชั้นความลับข้อมูลดำเนินการโดยทีมบริการข้อมูล และได้รับอนุมัติโดยคณะกรรมการธรรมาภิบาลข้อมูล
3. ในการประชุมคณะกรรมการธรรมาภิบาลข้อมูล จำเป็นต้องบรรจุวาระเกี่ยวกับการทบทวนระดับชั้นความลับข้อมูล อย่างน้อยปีละ 1 ครั้ง
4. ทุกฟิลดในแต่ละชุดข้อมูลถือว่ามึระดับชั้นความลับเท่ากัน สำหรับชุดข้อมูลที่มีระดับความลับ เป็นระดับที่ 2 ระดับที่ 3 หรือ ระดับที่ 4 จำเป็นต้องระบุสิทธิในการเข้าถึงข้อมูลภายในองค์กรด้วย
5. การเผยแพร่ข้อมูลระดับที่ 1 ต้องได้รับการอนุมัติจากผู้บริหารระดับสูงด้านข้อมูล
6. ข้อมูลระดับที่ 2 เป็นต้นไปจะต้องมีกระบวนการในการร้องขอข้อมูล
7. บุคคลเจ้าของข้อมูล มีหน้าที่ร่วมพิจารณาและรับทราบการร้องขอข้อมูลส่วนบุคคล
8. เจ้าของข้อมูล มีหน้าที่พิจารณาอนุมัติการร้องขอข้อมูลร่วมกับบริการข้อมูล และตรวจสอบ ทบทวนการ จัดลำดับชั้นความลับข้อมูล
9. บริการข้อมูล มีหน้าที่ตรวจสอบการใช้งานข้อมูลสาธารณะและประเมินผลกระทบของการ คุ้มครองข้อมูล (Data Protection Impact Assessment: DPIA)
10. เจ้าของข้อมูลทำหน้าที่อนุมัติการร้องขอข้อมูลร่วมกับบริการข้อมูล
11. ในกรณีที่ผู้ร้องขอข้อมูลไม่มีสิทธิตามสิทธิการเข้าถึงข้อมูล จำเป็นต้องดำเนินการตาม กระบวนการดังต่อไปนี้
 - 11.1 ข้อมูลส่วนบุคคล ต้องมีการร้องขอผ่านส่วนงานที่บุคคลนั้นสังกัด โดยแจ้งวัตถุประสงค์ให้ชัดเจนโดยบุคคลเจ้าของข้อมูล และบริการข้อมูลของฝ่ายทรัพยากรบุคคลต้องรับทราบและมีสิทธิที่จะปฏิเสธการร้องขอนั้นเว้นแต่จะมีประกาศของ สนพ. รองรับ

11.2 ข้อมูลความลับทางราชการ ต้องมีการร้องขอผ่านส่วนงานที่เป็นเจ้าของข้อมูล โดยเจ้าของข้อมูล และบริการข้อมูลแต่ละกอง/ศูนย์/กลุ่มงานต้องพิจารณาร่วมกัน ถ้าเป็นข้อมูลที่มีความอ่อนไหว หรือมีความเสี่ยงต้องได้รับการอนุมัติโดยคณะกรรมการธรรมาภิบาลข้อมูล

11.3 ข้อมูลความมั่นคง ต้องมีการร้องขอผ่านส่วนงานที่เป็นเจ้าของข้อมูล โดยต้องได้รับการอนุมัติจากคณะกรรมการธรรมาภิบาลข้อมูลเท่านั้น

12. ระดับชั้นความลับข้อมูลจะต้องถูกระบุไว้ในคำอธิบายชุดข้อมูล (Metadata)

13. การร้องขอข้อมูลต้องมีการเก็บบันทึกด้วย

ส่วนที่ 5

นโยบายและแนวปฏิบัติกระบวนการจัดการข้อมูลตามวงจรชีวิตข้อมูล

วัตถุประสงค์

เพื่อให้การบริหารจัดการชุดข้อมูลของ สนพ. มีประสิทธิภาพและเกิดประสิทธิผลในการนำไปใช้ประโยชน์

แนวปฏิบัติ

1. การสร้างข้อมูล (Create)
 - 1.1 กำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน หรือสร้างข้อมูลตามมาตรฐานที่เกี่ยวข้อง
 - 1.2 กำหนดหน้าที่ความรับผิดชอบในการนำเข้าข้อมูล และการเข้าถึงข้อมูล
 - 1.3 กำหนดสิทธิการเข้าถึงข้อมูล วิธีและเครื่องมือที่ใช้ในการเข้าถึงข้อมูล
 - 1.4 กำหนดระยะเวลาในการทบทวนสิทธิ และวิธีในการเข้าถึงข้อมูล
 - 1.5 ให้องค์กรที่สร้างข้อมูลตรวจสอบ และบันทึกข้อมูลตั้งต้นให้ถูกต้อง ครบถ้วน ตรงกับข้อเท็จจริง โดยมีการบันทึกข้อมูลและจัดเก็บตามขั้นตอนการรักษาความปลอดภัย
2. การรวบรวมและการจัดเก็บข้อมูล (Collect/Store)
 - 2.1 การรวบรวมและจัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน และจัดทำเมทาดาทาสำหรับชุดข้อมูลที่มีการจัดเก็บอยู่ในฐานข้อมูล
 - 2.2 กรณีเป็นการจัดเก็บข้อมูลส่วนบุคคล ต้องมีการแจ้งหรือขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล และเลือกใช้ฐานกฎหมายตามความเหมาะสมเพื่อให้เป็นไปตามนโยบายข้อมูลส่วนบุคคลขององค์กร
 - 2.3 กำหนดกระบวนการทดสอบข้อมูลที่จัดเก็บให้มีความถูกต้องและครบถ้วน
 - 2.4 กำหนดมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลต่างๆ อย่างเหมาะสม
 - 2.5 กำหนดความต้องการหรือคุณลักษณะของระบบจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัย และคุณภาพของข้อมูล
 - 2.6 กำหนดการสำรองข้อมูลหากเกิดเหตุฉุกเฉิน เพื่อให้สามารถใช้งานข้อมูลได้อย่างต่อเนื่อง
3. การคัดแยกข้อมูล (Classify)
 - 3.1 กำหนดเงื่อนไขในการเผยแพร่ข้อมูลสำหรับผู้ภายในและภายนอกให้ชัดเจน
 - 3.2 ลดความยุ่งยากและซับซ้อนในการเปิดเผยข้อมูลให้เหลือน้อยที่สุด
4. การประมวลผลหรือใช้ข้อมูล (Process/Use)
 - 4.1 กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และสื่อสารให้ผู้ที่เกี่ยวข้องทราบ
 - 4.2 การประมวลผลข้อมูลที่เป็นความลับ ให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ที่ประกาศไว้อย่างเคร่งครัด
 - 4.3 กำหนดกระบวนการ และเทคโนโลยีในการแลกเปลี่ยน/เชื่อมโยงข้อมูลให้ชัดเจน ตั้งแต่ขั้นตอนการเตรียมการ เริ่มดำเนินการ ระหว่างดำเนินการ และสิ้นสุดการดำเนินการให้เป็นไปตามมาตรฐานที่เกี่ยวข้อง

5. การปกปิดหรือเปิดเผยข้อมูล (Concealment/Disclosure)

5.1 การกำหนดชั้นความลับของข้อมูลต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของ ประเทศ ความลับทางราชการ ความเป็นส่วนบุคคล ฯลฯ และต้องตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูล ไปใช้ตามบทบาทและภารกิจตามกฎหมายของหน่วยงานนั้นๆ เพื่อเป็นการรักษาคุณภาพและความมั่นคงปลอดภัย ของข้อมูล

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 กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของระบบที่ใช้ใน การให้บริการหรือระบบงานสารสนเทศอย่างน้อยปีละ 1 ครั้ง

6.2 ต้องสามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมเป็นไปตามแนวทาง ที่กำหนดไว้

6.3 หากพบว่าข้อมูลที่จัดเก็บไม่ถูกต้องให้แจ้งเจ้าของข้อมูลเพื่อปรับปรุงแก้ไข

7. การทำลายข้อมูล (Destroy)

7.1 กำหนดระยะเวลาในการจัดเก็บข้อมูลที่เหมาะสมกับข้อมูลแต่ละประเภท

7.2 กำหนดอำนาจอนุมัติ สิทธิ และยืนยันตัวบุคคลในการทำลายข้อมูล

7.3 ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ผู้ควบคุมข้อมูลหรือ หน่วยงานที่จัดเก็บต้องดำเนินการให้เร็วที่สุด ทั้งนี้ต้องไม่ขัดต่อข้อตกลงระหว่างเจ้าของข้อมูลกับผู้ควบคุม ข้อมูล หรือกฎหมายใดๆ

7.4 กำหนดขั้นตอนและวิธีในการทำลายข้อมูล และเก็บรักษาคำอธิบายชุดข้อมูล (Metadata) ของข้อมูลที่ทำลายไว้เพื่อใช้สำหรับการตรวจสอบในภายหลัง

7.5 สร้างความรู้และความเข้าใจในการจัดเก็บและทำลายข้อมูลแก่ผู้ที่เกี่ยวข้อง

ส่วนที่ 6

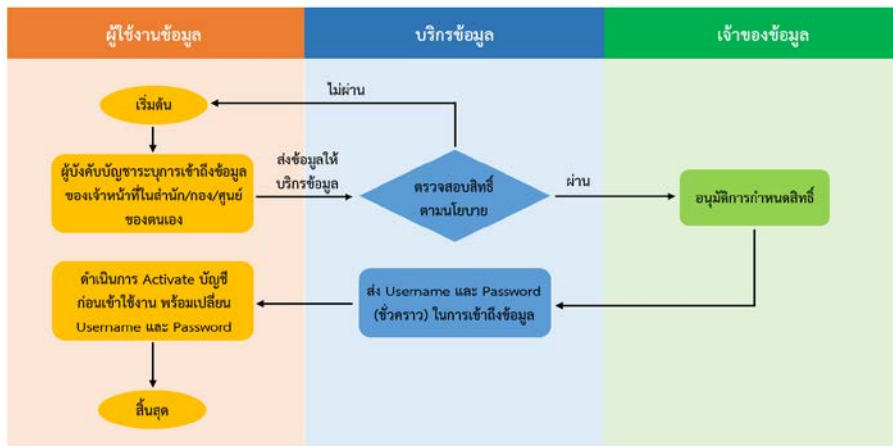
สิทธิการเข้าถึงข้อมูล

วัตถุประสงค์

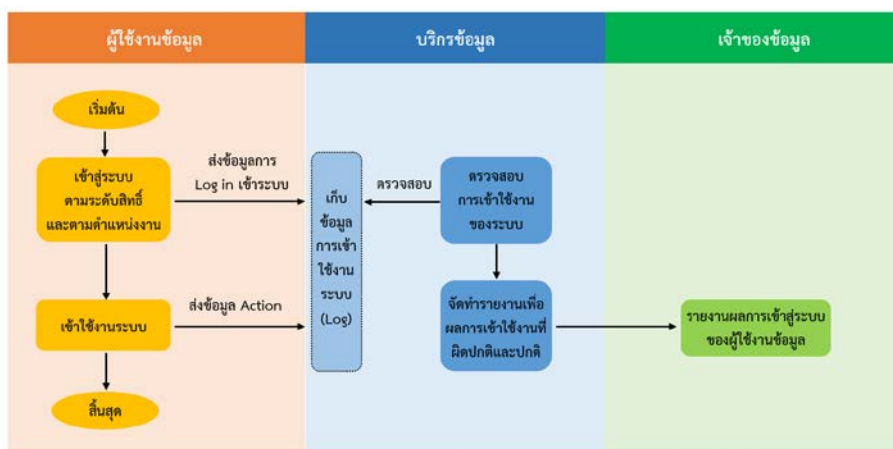
เพื่อกำหนดมาตรฐาน กระบวนการ บุคลากร หน้าที่และความรับผิดชอบ และเทคโนโลยีที่ สนพ. ต้องปฏิบัติในการกำหนดสิทธิการเข้าถึงข้อมูล

แนวปฏิบัติ

1. ทุกชุดข้อมูลต้องระบุสิทธิในการเข้าถึงข้อมูลเป็นเมทริกซ์ CRUD (Create – Read – Update – Delete) ในการระบุสิทธิการสร้าง เข้าถึงเพื่ออ่าน เข้าถึงเพื่อแก้ไข และหรือลบข้อมูล
2. สิทธิในการเข้าถึงข้อมูลกำหนดโดยตำแหน่งงาน
3. สิทธิในการเข้าระบบกำหนดเป็นรายบุคคล
4. ทุกแอปพลิเคชันหรือระบบต้องปฏิบัติตามสิทธิการเข้าถึงข้อมูล
5. บริการข้อมูล (สารสนเทศ) ทำการตรวจสอบการเข้าถึงข้อมูลในประเด็นการเข้าถึงที่ผิดนโยบาย หรือการเข้าถึงที่ผิดปกติที่มีความเสี่ยงต่อการโดนโจมตี และต้องรายงานต่อคณะกรรมการธรรมาภิบาลข้อมูล
6. ผู้ใช้งานข้อมูล ซึ่งนำเข้าข้อมูลปฏิบัติตามสิทธิการเข้าถึงข้อมูลที่คณะกรรมการธรรมาภิบาล กำหนด
7. คณะกรรมการธรรมาภิบาลข้อมูลเป็นผู้เห็นชอบการระบุสิทธิการเข้าถึงข้อมูลในฐานข้อมูลของแต่ละระบบ
8. ผู้ดูแลระบบไม่สามารถแก้ไขข้อมูลได้เอง การแก้ไขข้อมูลต้องผ่านการกลั่นกรองและเห็นชอบจาก คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ตามชั้นความลับ หรือระดับความสำคัญของ ผลกระทบ
9. บริการข้อมูลทุกส่วนงานต้องทำการระบุสิทธิเข้าถึงของข้อมูลตามตำแหน่งงาน ให้เป็นไปตามมาตรฐาน โดยกำกับดูแลความถูกต้องและตรวจสอบโดยฝ่ายสารสนเทศ
10. มีการทบทวนสิทธิการเข้าถึงข้อมูล อย่างน้อยปีละ 1 ครั้ง
11. การสร้างและการเข้าถึงข้อมูลในทุกกิจกรรมต้องมีการเก็บบันทึก
12. การระบุสิทธิของบุคลากรตามตำแหน่งต้องตั้งค่าใน Active Directory กระบวนการขอสิทธิการเข้าถึงข้อมูลและกระบวนการตรวจสอบสิทธิการเข้าถึงข้อมูล ดังแสดงในภาพที่ 6 และ 7 ตามลำดับ



ภาพที่ 6 กระบวนการขอสิทธิการเข้าถึงข้อมูล



ภาพที่ 7 กระบวนการตรวจสอบสิทธิการเข้าถึงข้อมูล

ส่วนที่ 7 คุณภาพข้อมูล

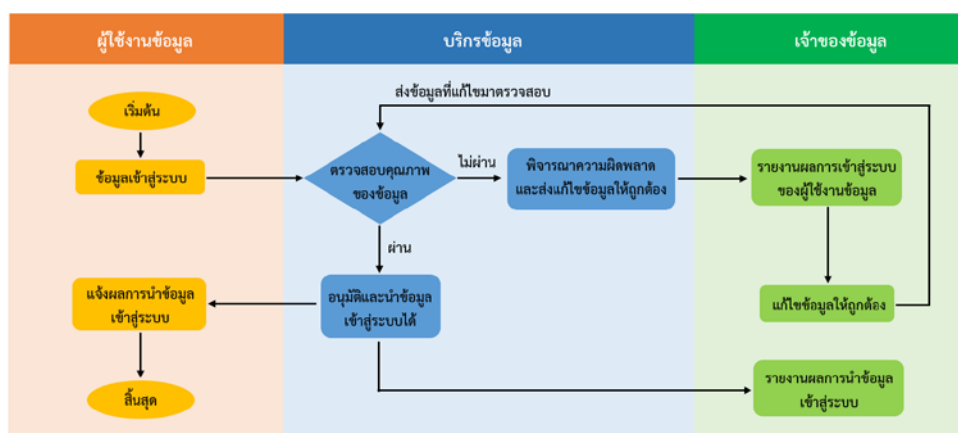
วัตถุประสงค์

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

แนวปฏิบัติ

1. ชุดข้อมูลทุกชุดต้องมีคุณภาพข้อมูลอย่างน้อยครอบคลุมถึงความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องกัน (Consistency) และความเป็นปัจจุบัน (Timeliness)
 - 1.1 ความถูกต้องของข้อมูลต้องมีการตรวจสอบโดยบริการข้อมูล และแก้ไขโดยเจ้าของข้อมูล
 - 1.2 ความครบถ้วนของข้อมูลสามารถตรวจสอบได้
 - 1.3 ความต้องกันของข้อมูลสามารถตรวจสอบได้กับมาตรฐานข้อมูลที่ตั้งไว้ในแต่ละชุดข้อมูล
 - 1.4 ความเป็นปัจจุบันต้องมีการเปรียบเทียบกับฟิลด์อ้างอิงที่เป็นเกณฑ์เวลาตามมาตรฐาน
2. คุณภาพข้อมูลต้องดำเนินการโดยเจ้าของข้อมูล ผู้ใช้ข้อมูล และบริการข้อมูลในสำนัก/กอง/ศูนย์/กลุ่มงาน และเห็นชอบโดยคณะกรรมการธรรมาภิบาลข้อมูล
3. คุณภาพข้อมูลจะต้องแนบไปกับการใช้ข้อมูลและคำอธิบายชุดข้อมูล (Metadata)
4. คุณภาพข้อมูลต้องมีการทบทวนอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง
5. เมื่อมีการนำเข้าข้อมูล ผู้ใช้ข้อมูลมีหน้าที่ตรวจสอบคุณภาพข้อมูลก่อนนำเข้า
6. เมื่อข้อมูลถูกนำเข้าไปแล้ว บริการข้อมูลแต่ละสำนัก/กอง/ศูนย์/กลุ่มงาน จะทำการตรวจสอบคุณภาพข้อมูลโดยรวมอีกครั้ง ถ้ามีความผิดพลาด บริการข้อมูลจะต้องแจ้งไปยังเจ้าของข้อมูลให้รับทราบ และแจ้งให้เจ้าของข้อมูลนำเข้าข้อมูลดำเนินการแก้ไข
7. ถ้ามีความจำเป็นต้องทบทวนนโยบายให้นำเรื่องเข้าสู่การประชุมของคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)

กระบวนการตรวจสอบคุณภาพข้อมูลดังแสดงในภาพที่ 8



ภาพที่ 8 กระบวนการตรวจสอบคุณภาพข้อมูล

ส่วนที่ 8

การปฏิบัติงานตามหลักธรรมาภิบาลข้อมูล

วัตถุประสงค์

เพื่อระบุบทบาทหน้าที่ของบุคลากรที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล

การปฏิบัติหน้าที่

- คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของ สนพ. มีหน้าที่รับผิดชอบ ดังนี้
 - กำหนดความต้องการ ให้ข้อเสนอแนะ และอนุมัติ นโยบาย ข้อมูล คุณภาพ ความมั่นคงปลอดภัย ชั้นความลับ ระเบียบ และข้อบังคับอื่นๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการจัดลำดับความสำคัญของข้อมูลในการดำเนินการธรรมาภิบาลข้อมูล
 - ให้ความเห็นและข้อเสนอแนะในด้านการจัดการและการกำกับดูแลข้อมูลต่อบริการข้อมูล มีส่วนร่วมในการให้การสนับสนุนและพิจารณาโยบายด้านข้อมูล และให้การสนับสนุนทรัพยากรจาก แต่ละกอง/ศูนย์/กลุ่มงาน เพื่อดำเนินงานตามนโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูล
 - นำข้อมูลและวิเคราะห์ข้อมูล เพื่อจัดทำยุทธศาสตร์และดำเนินการกำกับดูแลข้อมูลให้มี คุณภาพ นำแนวปฏิบัติและมาตรฐานของหน่วยงานไปปรับปรุง รวมถึงทบทวนและติดตามการดำเนินงานธรรมาภิบาลข้อมูล
 - เป็นตัวกลางระหว่างหน่วยงานภาครัฐในการเชื่อมโยงและแลกเปลี่ยนข้อมูล ให้ข้อมูลของหน่วยงานมีคุณภาพ และเกิดประโยชน์สูงสุดต่อหน่วยงาน
 - เลขานุการมีหน้าที่ประสานงานกับสำนัก/กอง/ศูนย์/กลุ่มงานต่างๆ ในด้านการจัดประชุม การดำเนินงานตามนโยบาย ประสานกับบริการข้อมูลในการนำประเด็นปัญหาที่พบ หรือข้อเสนอแนะจากผู้ใช้อข้อมูล หรือเจ้าของข้อมูลมาพิจารณาในคณะกรรมการธรรมาภิบาลข้อมูล
 - ต้องจัดหาหลักสูตรฝึกอบรมสำหรับบุคลากร สนพ. ทุกท่าน รวมถึงต้องมีการจัดหลักสูตร อบรมให้ทันสมัยทุก 1 ปี
 - เผยแพร่ข้อสรุป มาตรฐาน หรือนโยบายที่มีการอนุมัติจากที่ประชุมคณะกรรมการธรรมาภิบาลข้อมูลให้บุคลากร สนพ. ได้รับทราบ
 - ต้องจัดประชุมอย่างน้อยปีละ 1 ครั้ง เพื่อรับทราบปัญหา ทบทวน แก้ไขนโยบายและตัดสินใจด้านข้อมูล
- บริการข้อมูล มีหน้าที่รับผิดชอบ คือ
 - ดำเนินการกำกับดูแล ติดตาม และรายงานผลการดำเนินการธรรมาภิบาลข้อมูล
 - นิยามข้อมูล นิยามความต้องการด้านคุณภาพ และความมั่นคงปลอดภัยร่วมกับเจ้าของข้อมูล
 - บริหารจัดการ ควบคุมการดำเนินงานตามนโยบายจากคณะกรรมการธรรมาภิบาลข้อมูล ติดตามการดำเนินงานและข้อเสนอแนะเพื่อเป็นข้อมูลให้แก่ผู้บริหารระดับสูงด้านข้อมูล หรือคณะกรรมการธรรมาภิบาลข้อมูล
 - ตรวจสอบความสอดคล้องกันระหว่างนโยบายกับการดำเนินการต่อข้อมูล ตรวจสอบ คุณภาพ ข้อมูล วิเคราะห์ผลจากการตรวจสอบ และรายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและ ผู้ที่เกี่ยวข้องอื่นๆ
 - ประสานงานในปัญหาด้านข้อมูลจากบุคลากรในส่วนงานเดียวกัน
- เจ้าของข้อมูล มีหน้าที่

3.1 ตรวจสอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการ ข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบหรือกฎหมาย

3.2 ทบทวนและร่วมอนุมัติการดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูล

3.3 ดำเนินงานตรวจสอบคุณภาพข้อมูลและการเชื่อมโยงข้อมูลร่วมกับบริการข้อมูล

3.4 ระบุสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูลเพื่อให้คณะกรรมการธรรมาภิบาล ข้อมูลอนุมัติ

3.5 เป็นผู้ควบคุมการดำเนินงานของผู้ใช้ข้อมูล

4. ผู้สร้างข้อมูล มีหน้าที่

4.1 บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกต้องไว้

4.2 ทำงานร่วมกับบริการข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูล และความมั่นคง ปลอดภัยของข้อมูล

ส่วนที่ 9 กฎ ระเบียบที่เกี่ยวข้อง

วัตถุประสงค์

เพื่ออ้างอิงกฎหมาย ระเบียบ ข้อบังคับ นโยบาย และแนวปฏิบัติที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ

แนวปฏิบัติ

1. การเปิดเผยข้อมูล

การเปิดเผยข้อมูลเป็นสิ่งจำเป็นต่อการดำเนินงานของหน่วยงานภาครัฐ เพื่อแสดงถึงความโปร่งใสในการดำเนินงาน และความสามารถในการตรวจสอบได้จากผู้ที่มีส่วนได้ส่วนเสียทุกภาคส่วน รวมถึงเป็นการสนับสนุนให้มีการนำข้อมูลที่เปิดเผยไปสร้างนวัตกรรมผลิตภัณฑ์และบริการเพื่อยกระดับการพัฒนาประเทศ ทั้งนี้ กฎหมายที่เกี่ยวข้องกับการเปิดเผยข้อมูลมีดังนี้

1.1 รัฐธรรมนูญแห่งราชอาณาจักรไทยพุทธศักราช 2560 ในมาตราที่ 59 ได้ระบุว่า รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐที่มีใช้ข้อมูลเกี่ยวกับความมั่นคงของรัฐหรือเป็นความลับของทางราชการ

1.2 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ให้มีการเปิดเผยข้อมูลหรือข่าวสารสาธารณะที่หน่วยงานของรัฐจัดทำและครอบครองในรูปแบบและช่องทางดิจิทัล เพื่อให้ประชาชนเข้าถึงโดยสะดวก มีส่วนร่วมและตรวจสอบการดำเนินงานของรัฐ และสามารถนำข้อมูล ไปพัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่างๆ

1.3 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 มี 3 ประเด็นที่เกี่ยวข้องกับการเปิดเผยข้อมูล ได้แก่

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

2. การเชื่อมโยงและแลกเปลี่ยนข้อมูล

การเชื่อมโยงและแลกเปลี่ยนข้อมูลเป็นสิ่งสำคัญต่อการบูรณาการการดำเนินงานระหว่างหน่วยงานภาครัฐ และเป็นประโยชน์ในการขอใช้บริการจากประชาชนหรือหน่วยงานที่เกี่ยวข้อง โดยกฎหมายที่เกี่ยวข้อง คือ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ที่กำหนดให้มีการพัฒนามาตรฐาน หลักเกณฑ์ และวิธีการเกี่ยวกับดิจิทัล และพัฒนาโครงสร้างพื้นฐาน ด้านดิจิทัลที่จำเป็น ให้เป็นไปตามมาตรฐานสากล เพื่อสร้างและพัฒนาระบบการทำงานของหน่วยงานของรัฐให้มีความสอดคล้องและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกัน รวมทั้งมีความมั่นคงปลอดภัยและน่าเชื่อถือ โดยมีการบูรณาการและสามารถทำงานร่วมกันอย่างเป็นเอกภาพ เกิดการพัฒนาการบริการภาครัฐที่มีประสิทธิภาพและนำไปสู่การบริหารราชการและการบริการประชาชนแบบบูรณาการ เพื่อให้เข้าถึงบริการได้อย่างสะดวก

3. การคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคล (Privacy Data Protection) เป็นสิ่งสำคัญที่ภาครัฐต้องดำเนินการ โดยจะต้องมีการรวบรวม จัดเก็บ ใช้หรือเผยแพร่ข้อมูลส่วนบุคคลของผู้ใช้บริการในรูปแบบของข้อมูล

อิเล็กทรอนิกส์เพื่อป้องกันการละเมิดข้อมูลส่วนบุคคล และสร้างความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์ของประชาชน โดยมีกฎหมายที่เกี่ยวข้อง ดังนี้

3.1 พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 กำหนดประเภทข้อมูลที่เปิดเผยได้ และเปิดเผยไม่ได้ ซึ่งจะต้องมีการพิจารณาในกรณีที่เป็นข้อมูลส่วนบุคคลที่ต้องได้รับการคุ้มครองอย่างมีหลักเกณฑ์

3.2 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการกำหนดหลักเกณฑ์ กลไก และมาตรการที่กำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

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

4. การรักษาความลับ

การรักษาความลับทางราชการเป็นสิ่งจำเป็นต่อการดำเนินงานของหน่วยงาน เพื่อเป็นการป้องกันความเสียหายที่จะเกิดขึ้นต่อภาครัฐ ทั้งในด้านชื่อเสียง การเงิน ความสามารถในการพัฒนาประเทศ และความมั่นคงของประเทศ โดยมีกฎหมายและระเบียบที่เกี่ยวข้อง ดังนี้

4.1 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม ได้มีข้อกำหนดที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ ได้แก่ กำหนดนิยามข้อมูลข่าวสารลับ และกำหนดหลักเกณฑ์และวิธีการในการรักษาความลับของหน่วยงานภาครัฐ

4.2 แนวทางปฏิบัติในการรักษาความปลอดภัยเกี่ยวกับบุคคล เอกสาร และสถานที่ที่จัดทำขึ้นจากระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552

5. ประเด็นอื่นๆ ที่เกี่ยวข้องกับเรื่องธรรมาภิบาลข้อมูลภาครัฐ

5.1 พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 กำหนดให้หน่วยงานรัฐจัดให้มีการบริหารงานและการจัดทำบริการสาธารณะในรูปแบบและช่องทางดิจิทัล โดยมีการบริหารจัดการและบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล โดยมุ่งหมายในการเพิ่มประสิทธิภาพและอำนวยความสะดวกในการให้บริการและเข้าถึงประชาชน และในการเปิดเผยข้อมูลภาครัฐต่อสาธารณะและสร้างการมีส่วนร่วม ของทุกภาคส่วน

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

5.3 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555 โดยกำหนดให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยการเข้าถึงข้อมูลสารสนเทศ ในระดับเคร่งครัด ระดับกลาง หรือระดับพื้นฐาน ให้หน่วยงานหรือองค์กรหรือส่วนงานของหน่วยงานหรือองค์กรปฏิบัติตามมาตรฐาน