สำนักงานนวัตกรรมแห่งชาติ

นโยบายและแนวปฏิบัติ
ด้านธรรมาภิบาลข้อมูล

Data Governance

สำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน)
ฝ่ายบริหารองค์กร
งานเทคโนโลยีสารสนเทศ

บทนำ

ข้อมูลของสำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) เป็นข้อมูลด้านนวัตกรรมที่สำคัญของประเทศ โดยมีการให้บริการกับหน่วยงานภาครัฐ หน่วยงานเอกชนและประชาชนในวงกว้าง ดังนั้น จึงต้องมีธรรมาภิบาลข้อมูลและการกำกับดูแลที่ดีเพื่อให้ข้อมูลมีคุณภาพ พร้อมใช้ มีความเชื่อมโยงกัน และมีความปลอดภัย อันเป็นการสร้างประโยชน์ในเชิงเศรษฐกิจให้กับประเทศอย่างยั่งยืน

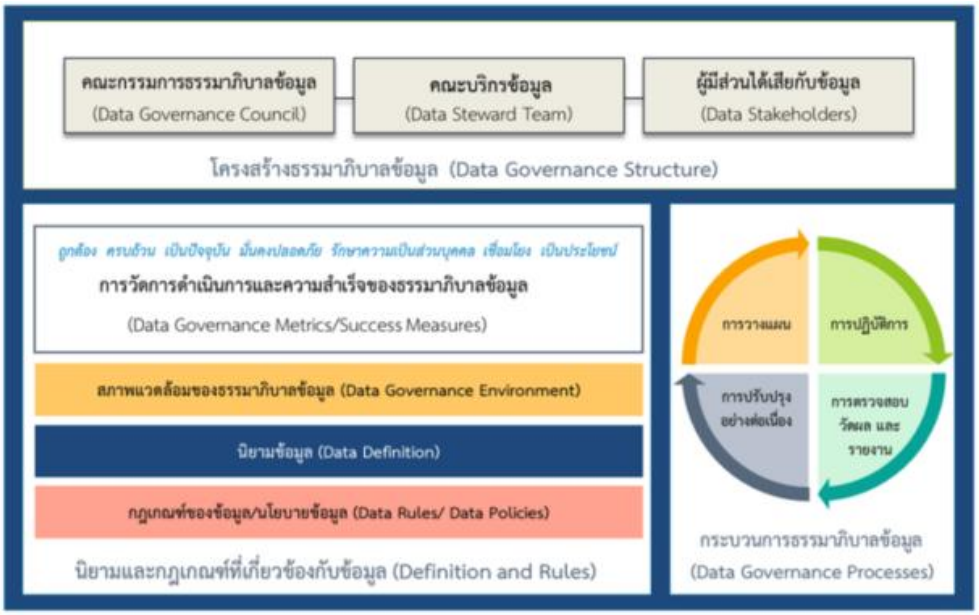
สำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) ได้นำแนวทางตามกรอบธรรมาภิบาลข้อมูล ที่ประกอบด้วยองค์ประกอบต่าง ๆ ผนวกเข้าด้วยกัน ทั้งในด้านของนิยามและกฎเกณฑ์ที่เกี่ยวข้องกับข้อมูล บุคคล และกระบวนการ ซึ่งองค์ประกอบเหล่านี้มีความสำคัญที่ก่อให้เกิดประสิทธิภาพและประสิทธิผลในการดำเนินงาน อันจะนำไปสู่การบรรลุเป้าหมายในการดำเนินงานตามที่กำหนดไว้ ซึ่งโครงสร้างธรรมาภิบาลข้อมูล (Data Governance Structure) ประกอบด้วย

(1) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)

(2) คณะบริกรข้อมูล (Data Steward Team) และ

(3) ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)

โดยมีกระบวนการธรรมาภิบาลข้อมูล (Data Governance Processes) มากำกับดูแลการดำเนินการหรือกิจกรรม ตลอดจนบุคคล ที่เกี่ยวข้องกับโครงสร้างธรรมาภิบาลข้อมูล จะถูกแต่งตั้งโดยกรม เพื่อทำหน้าที่กำหนดยุทธศาสตร์และเป้าหมาย ตรวจสอบสภาพแวดล้อมของธรรมาภิบาลข้อมูล นิยาม ความหมายและขอบเขตของข้อมูล กำหนดกฎเกณฑ์และนโยบายข้อมูล (Definition and Rules) และดำเนินการตรวจสอบการปฏิบัติตามกฎเกณฑ์และนโยบายข้อมูล มีการรายงานไปยังผู้บริหาร เพื่อปรับปรุงกฎเกณฑ์ นโยบายการดำเนินงานให้ถูกต้อง เหมาะสมต่อไป



ธรรมาภิบาลข้อมูลสำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) ประกอบด้วยเนื้อหา 6 ส่วน โดยสอดคล้องกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูล ดังนี้

1. สิทธิหน้าที่และความรับผิดชอบของผู้ซึ่งมีหน้าที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของหน่วยงาน (Roles and Responsibilities)
2. กระบวนการธรรมาภิบาลข้อมูล (Data Governance Processes)

3. มาตรการควบคุม (Controls)
4. การวัดผลการบริหารจัดการข้อมูล (Data Management Measurements)
5. การจำแนกหมวดหมู่ของข้อมูล (Data Categories)
6. คำอธิบายชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata)

1. สิทธิหน้าที่ และความรับผิดชอบของผู้ซึ่งมีหน้าที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของหน่วยงาน (Roles and Responsibilities)

คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของสำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) ประกอบด้วย ผู้อำนวยการสำนักงานนวัตกรรมแห่งชาติและผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) เป็นประธานคณะกรรมการ และรองผู้อำนวยการและผู้อำนวยการฝ่าย เป็นกรรมการ ซึ่งคณะกรรมการมีอำนาจสูงสุดในธรรมาภิบาลข้อมูลของกรม ทำหน้าที่ตัดสินใจเชิงนโยบาย แก้ไขปัญหา และบริหารจัดการธรรมาภิบาลข้อมูล ร่วมกับทีมบริกรข้อมูล (Data Steward Team)

1.1 โครงสร้างบุคลากร

โครงสร้างบุคลากรด้านธรรมาภิบาลข้อมูล มีรายละเอียด ดังนี้

1) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ประกอบด้วย ประธานกรรมการและกรรมการ ได้แก่ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) ผู้อำนวยการ ผู้เชี่ยวชาญ หรือหัวหน้าส่วนที่เกี่ยวข้อง
2) คณะบริกรข้อมูล (Data Steward Team)
   2.1) หัวหน้าคณะบริกรข้อมูล (Lead Data Steward) ได้แก่ ผู้อำนวยการฝ่ายยุทธศาสตร์นวัตกรรม
   2.2) ผู้แทนจากงานต่างๆ ที่เกี่ยวข้อง ดังนี้
      2.2.1) บริกรข้อมูลด้านธุรกิจ (Business Data Stewards)
      2.2.2) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards)
      2.2.3) บริกรข้อมูลด้านคุณภาพข้อมูล (Quality Data Stewards)

นอกเหนือจากคณะกรรมการและทีมบริกรข้อมูล ยังมีผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders) อื่น ๆ เช่น ผู้บริหารจัดการข้อมูลเชิงเทคนิค ผู้บริหารจัดการข้อมูลเชิงธุรกิจ เจ้าของข้อมูล (Data Owners) ผู้บริหารจัดการข้อมูล (Data Management Team) ผู้สร้างข้อมูล (Data Creators) และผู้ใช้ข้อมูล (Data Users)

1.2 บทบาทและความรับผิดชอบ (Roles and Responsibilities)

บทบาท (Roles) และความรับผิดชอบ (Responsibilities) ในแต่ละส่วนที่อยู่ในโครงสร้างบุคลากรด้านธรรมาภิบาลข้อมูลของกรม ดังนี้

1) คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)

มีอำนาจหน้าที่ ดังนี้

(1) จัดทำธรรมาภิบาลข้อมูลของสำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) โดยกำหนดนโยบายข้อมูลและแนวทางปฏิบัติงาน ให้สอดคล้องกับภารกิจขององค์กรและเป็นไปตาม

กรอบธรรมาภิบาลข้อมูล รวมทั้งควบคุมการดำเนินงาน ทบทวนและปรับปรุงธรรมาภิบาลข้อมูลให้มีความเหมาะสมอย่างต่อเนื่อง

(2) อนุมัติมาตรฐานข้อมูล เกณฑ์การวัดคุณภาพ ระเบียบ และข้อบังคับอื่นๆ ที่เกี่ยวข้องกับข้อมูล ตลอดจนให้ข้อเสนอแนะ รวมทั้งจัดลำดับความสำคัญและแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล เพื่อรักษาความสมบูรณ์ของข้อมูลหน่วยงานภาครัฐ และเพื่อให้การดำเนินการธรรมาภิบาลข้อมูลเป็นไปอย่างมีประสิทธิภาพ

(3) เป็นตัวกลางระหว่างหน่วยงานภาครัฐในการแลกเปลี่ยน เชื่อมโยงข้อมูลและจัดการความเสี่ยงที่อาจเกิดจากข้อมูลของหน่วยงานภาครัฐ

(4) จัดหาเทคโนโลยีที่ทันสมัยเพื่อนำมาวิเคราะห์ข้อมูล รวมทั้งส่งเสริมนวัตกรรมที่ใช้ประโยชน์จากข้อมูลในการวิเคราะห์เพื่อแก้ไขและลดความเสี่ยงของปัญหาที่อาจเกิดขึ้นในอนาคต เพื่อให้ข้อมูลของหน่วยงานภาครัฐมีคุณค่าและเกิดประโยชน์สูงสุด

(5) แต่งตั้งคณะบริกรข้อมูลหรือคณะทำงาน เพื่อให้การดำเนินการเป็นไปตามกรอบธรรมาภิบาลข้อมูล

(6) กำกับดูแลและสนับสนุนการดำเนินงานของคณะบริกรข้อมูลหรือคณะทำงานที่แต่งตั้ง

(7) ประสานหรือเชิญหน่วยงานที่เกี่ยวข้องเข้าร่วมประชุมหารือ ตลอดจนให้ความเห็นหรือคำแนะนำ

(8) ปฏิบัติงานอื่นใดตามที่ผู้อำนวยการสำนักงานนวัตกรรมแห่งชาติมอบหมาย

2) คณะบริกรข้อมูล (Data Steward Team)

2.1) หัวหน้าคณะบริกรข้อมูล (Lead Data Steward) มีอำนาจหน้าที่ในการกำกับดูแลและสนับสนุนการดำเนินงานของคณะบริกรข้อมูล ให้เป็นไปตามกรอบธรรมาภิบาลข้อมูล

2.2) บริกรข้อมูลด้านธุรกิจ (Business Data Stewards) คือ บุคคลที่ทำหน้าที่รับผิดชอบในการนิยามความต้องการด้านคุณภาพและความมั่นคงปลอดภัยซึ่งอาจจะได้รับมาจากผู้ใช้ข้อมูล (Data Users) หรือผู้มีส่วนได้เสียอื่น ๆ โดยส่วนใหญ่เป็นบุคคลที่มาจากฝ่ายธุรกิจแต่มีความเข้าใจด้านเทคโนโลยีสารสนเทศ

2.3) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) คือ บุคคลที่ทำหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศแก่บริกรข้อมูลด้านธุรกิจ ให้ข้อเสนอแนะเชิงเทคนิคในการร่างนโยบายข้อมูล ตรวจสอบคุณภาพข้อมูลความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายข้อมูลในเชิงเทคนิค ทั้งนี้บริกรข้อมูลด้านเทคนิค ส่วนใหญ่เป็นบุคคลฝ่ายเทคโนโลยีสารสนเทศแต่มีความเข้าใจเกี่ยวกับธุรกิจ

2.4) บริกรข้อมูลด้านคุณภาพ (Quality Data Stewards) คือ บุคคลที่ทำหน้าที่ดำเนินการในเรื่องคุณภาพข้อมูล เช่น กำหนดนโยบายข้อมูลด้านคุณภาพ การตรวจวัดคุณภาพข้อมูล และการวิเคราะห์คุณภาพข้อมูล

มีอำนาจหน้าที่ ดังนี้

(1) จัดทำร่างธรรมาภิบาลข้อมูล โดยกำหนดนโยบายข้อมูล จำแนกหมวดหมู่ของข้อมูล มาตรการควบคุมและพัฒนาคุณภาพข้อมูล เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัยและไม่ละเมิดความเป็นส่วนบุคคล รวมทั้งสามารถเชื่อมโยงข้อมูลแลกเปลี่ยนบูรณาการและใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

(2) กำหนดความต้องการด้านคุณภาพข้อมูลและความมั่นคงปลอดภัยจากผู้ใช้ข้อมูลหรือผู้มีส่วนได้เสียกับข้อมูล

(3) กำหนดนิยามพร้อมจัดทำคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาและบัญชีข้อมูล ให้ครบถ้วน ตามความจำเป็นในการใช้งานและตรงตามความต้องการของผู้มีส่วนได้เสียกับข้อมูล

(4) ดำเนินงานให้สอดคล้องกับนโยบาย เป้าประสงค์ ความต้องการของผู้มีส่วนได้เสียกับข้อมูล รวมทั้ง ติดตามการดำเนินงานตามแผนที่กำหนด ตรวจสอบการปฏิบัติตามนโยบายข้อมูล

(5) ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศ ในการจัดทำและให้ข้อเสนอแนะเชิงเทคนิคที่สอดคล้องนโยบาย เป้าประสงค์ความต้องการของผู้มีส่วนได้เสียกับข้อมูล

(6) กำหนดรายละเอียดที่เกี่ยวข้องกับการออกแบบระบบเทคโนโลยีสารสนเทศรวมถึงโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ เพื่อคุ้มครองข้อมูลและรักษาความมั่นคงปลอดภัย

(7) วิเคราะห์ความพร้อมของธรรมาภิบาลข้อมูล ความต้องการด้านคุณภาพข้อมูลการรักษาความเป็นส่วนบุคคลและความมั่นคงปลอดภัย ให้เหมาะสมกับสถานการณ์ปัจจุบัน เพื่อวางแผนการวัดและประเมินผล

(9) ตรวจสอบวิเคราะห์วัดผลการดำเนินงาน

(10) ทบทวนและปรับปรุงกระบวนการ เพื่อนำมาปรับปรุงกระบวนการทำงาน

(11) สนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศและอื่นๆ ที่เกี่ยวข้อง

(12) รายงานผลลัพธ์ไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้อง

(13) ปฏิบัติงานอื่นตามที่ได้รับมอบหมาย

3) ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholders)

คือ ผู้บริหารจัดการข้อมูลที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลภาครัฐ หรือผู้ที่มีส่วนเกี่ยวข้องกับข้อมูล โดยได้รับผลกระทบทางตรงหรือทางอ้อมจากการใช้บริการข้อมูล ซึ่งมีหน้าที่ให้การสนับสนุนการกำกับดูแลข้อมูลต่อคณะกรรมการธรรมาภิบาลข้อมูล ประกอบด้วย

3.1) ด้านการบริหารจัดการข้อมูล

3.1.1) **ผู้บริหารจัดการข้อมูลเชิงเทคนิค** ประกอบด้วย เจ้าหน้าที่เทคโนโลยีสารสนเทศ มีหน้าที่ความรับผิดชอบ คือ

- กำหนดโครงสร้างและความสัมพันธ์ของข้อมูล โดยพิจารณาจากความต้องการข้อมูล และวัตถุประสงค์ของหน่วยงาน
- พัฒนาสถาปัตยกรรมข้อมูลในภาพรวมของทั้งหน่วยงาน โดยประเมินสถานะในปัจจุบัน และออกแบบเพื่อปรับปรุงสำหรับอนาคต
- บริหารจัดการ และควบคุมเกี่ยวกับระบบฐานข้อมูลภายในหน่วยงาน
- กำหนดนโยบาย มาตรการ และมาตรฐานของระบบฐานข้อมูลทั้งหมดภายในหน่วยงาน เช่น รายละเอียดและวิธีการจัดเก็บข้อมูล การใช้งานฐานข้อมูล การรักษาความปลอดภัยของข้อมูล การสำรองข้อมูล การกู้คืนข้อมูล
- ออกแบบวิธีการจัดเก็บ และเรียกใช้งานข้อมูล
- จัดการเกี่ยวกับข้อมูลทั้งหมด ตั้งแต่ระบุชนิดของข้อมูล วางโครงสร้างของการเข้าและการออกของข้อมูล เพื่อให้ข้อมูลไหลได้อย่างไม่สะดุด

- วิเคราะห์และออกแบบระบบ โดยศึกษาเกี่ยวกับปัญหา รวบรวมความต้องการของผู้ใช้งานระบบ วิเคราะห์ระบบงานภายในหน่วยงาน
- ออกแบบจำลองข้อมูล เช่น Entity Relationship Diagram และ Data Flow Diagram
- ออกแบบและพัฒนาแบบจำลองข้อมูล (Data Model) เพื่ออธิบายลักษณะโครงสร้างและการทำงานของข้อมูลให้เห็นภาพได้มากขึ้น

3.1.2) **ผู้บริหารจัดการข้อมูลเชิงธุรกิจ** ประกอบด้วย นักพัฒนานวัตกรรมและนักส่งเสริมนวัตกรรม มีหน้าที่ความรับผิดชอบ คือ

- นำข้อมูลมาวิเคราะห์แนวโน้มในเชิงธุรกิจ หรือแก้ปัญหาจากสิ่งที่ผิดแปลกไปจากแนวโน้มเดิม โดยใช้ประสบการณ์ และหลักสถิติ
- ใช้โมเดลหรือเครื่องมือในการทำรายงาน เพื่อสรุปข้อมูลสำหรับใช้ในการตัดสินใจ
- นำข้อมูลจากหลายๆ แหล่ง และแปลงข้อมูล เพื่อหารูปแบบและความสัมพันธ์ของข้อมูล
- สร้างแบบจำลอง และดำเนินการกับข้อมูลด้วยวิธีการต่างๆ เช่น Machine Learning หรือเขียนโปรแกรม เพื่อทำนายมุมมอง และคำตอบใหม่ๆ
- ศึกษาและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับเทคโนโลยี กลยุทธ์ กลุ่มเป้าหมาย และหน่วยงานที่เกี่ยวข้อง
- ทำความเข้าใจเป้าหมายและปัญหาของหน่วยงาน วิเคราะห์ความต้องการ และหาคำตอบ เพื่อวางแผนด้านกลยุทธ์ และผลักดันให้เกิดการเปลี่ยนแปลง

3.2) ด้านธรรมาภิบาลข้อมูล

3.2.1) **เจ้าของข้อมูล (Data Owners)** คือ บุคคลหรือคณะบุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง เพื่อสร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบหรือกฎหมาย โดยเจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล นอกจากนี้ยังมีหน้าที่ในการให้สิทธิในการเข้าถึงข้อมูลและการจัดระดับชั้นข้อมูล โดยเจ้าของข้อมูลส่วนใหญ่อยู่ในตำแหน่งบริหาร ประกอบด้วย ผู้อำนวยการฝ่ายสนับสนุนการเงินนวัตกรรมที่จำเป็นต่อการพัฒนาประเทศ ผู้อำนวยการฝ่ายสนับสนุนการเงินนวัตกรรมรายพื้นที่ ผู้อำนวยการฝ่ายส่งเสริมวิสาหกิจเริ่มต้น ผู้อำนวยการฝ่ายส่งเสริมธุรกิจนวัตกรรม และฝ่ายงานภายใต้การกำกับดูแล งานสถาบันวิทยาการนวัตกรรม งานนวัตกรรมภูมิภาคและประเมินผล

3.2.2) **คณะบริหารจัดการข้อมูล (Data Management Team)** คือ บุคคลหรือคณะบุคคลที่มีหน้าที่หลักในการบริหารจัดการข้อมูล องค์ประกอบในการบริหารจัดการข้อมูล และสนับสนุนกิจกรรมของธรรมาภิบาลข้อมูลภาครัฐ ซึ่งเป็นเจ้าหน้าที่ในงานเทคโนโลยีสารสนเทศและเจ้าหน้าที่ในงานบริหารข้อมูลกลางและเชื่อมต่อผู้ประกอบการนวัตกรรม เพื่อให้กรมสามารถนำข้อมูลที่บริหารจัดการ ไป

ประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ ถูกต้อง เหมาะสม และสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของกรม

3.2.3) **ผู้สร้างข้อมูล (Data Creators)** คือ บุคคลที่ทำหน้าที่ บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับมาตรฐานที่กำหนด และยังมีหน้าที่ในการทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย ประกอบด้วย เจ้าหน้าที่ผู้ปฏิบัติงานภายใต้ ฝ่ายสนับสนุนการเงินนวัตกรรมที่จำเป็นต่อการพัฒนาประเทศ ฝ่ายการเงินนวัตกรรมรายพื้นที่ ฝ่ายส่งเสริมวิสาหกิจเริ่มต้น ฝ่ายส่งเสริมธุรกิจนวัตกรรม งานสถาบันวิทยาการนวัตกรรมและงานนวัตกรรมภูมิภาคและประเมินผล

3.2.4) **เจ้าหน้าที่ผู้รับผิดชอบดูแลข้อมูล (Data Agents)** คือ บุคคลที่มีหน้าที่จัดเก็บข้อมูลให้มั่นคงปลอดภัย รวมทั้งทบทวน หรือเสนออนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล และรายงานบันทึกกิจกรรมการประมวลผลข้อมูล ประกอบด้วย เจ้าหน้าที่ผู้ปฏิบัติงานภายใต้ ฝ่ายสนับสนุนการเงินนวัตกรรมที่จำเป็นต่อการพัฒนาประเทศ ฝ่ายการเงินนวัตกรรมรายพื้นที่ ฝ่ายส่งเสริมวิสาหกิจเริ่มต้น ฝ่ายส่งเสริมธุรกิจนวัตกรรม งานสถาบันวิทยาการนวัตกรรมและงานนวัตกรรมภูมิภาคและประเมินผล

3.2.5) **ผู้ใช้ข้อมูล (Data Users)** คือ บุคคลที่ทำหน้าที่นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร และสนับสนุนธรรมาภิบาลข้อมูลภาครัฐโดยการให้ความต้องการในการใช้ข้อมูล พร้อมทั้งรายงานประเด็นปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูลไปยังบริกรข้อมูล

3.2.6) **เจ้าของข้อมูลส่วนบุคคล (Data Subject)** คือ บุคคลธรรมดาที่ข้อมูลส่วนบุคคลเกี่ยวกับบุคคลนั้นระบุถึงได้ไม่ว่าทางตรงหรือทางอ้อม

2. กระบวนการธรรมาภิบาลข้อมูล (Data Governance Processes)

กระบวนการธรรมาภิบาลข้อมูลของกรมพัฒนาธุรกิจการค้า เป็นขั้นตอนที่ใช้สำหรับกำกับดูแลการดำเนินการใด ๆ ต่อข้อมูลให้เป็นไปตาม กฎ ระเบียบ ข้อบังคับ หรือนโยบายที่เกี่ยวข้องกับข้อมูล กระบวนการธรรมาภิบาลข้อมูล เริ่มตั้งแต่ 1) การวางแผน 2) การปฏิบัติการ 3) การตรวจสอบวัดผลและรายงาน และ 4) การปรับปรุงอย่างต่อเนื่อง รวมถึงกระบวนการจัดการด้านการสื่อสารระหว่าง 4 กิจกรรม ทั้งภายในองค์กรและภายนอกองค์กร โดยมีกระบวนการต่าง ๆ ดังนี้

2.1 การวางแผน (Plan)

สำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) ได้กำหนดวิสัยทัศน์ว่า “องค์กรหลักในการเสริมสร้างระบบนวัตกรรมแห่งชาติ เพื่อเพิ่มคุณค่าที่ยั่งยืน” โดยมี 5 ประเด็นหลักในการขับเคลื่อนองค์กร คือ 1) ส่งเสริม สนับสนุน และดำเนินการพัฒนานวัตกรรมของประเทศซึ่งรวมถึงการพัฒนา โครงการนวัตกรรมในระยะหลังการวิจัยและพัฒนา หรือการต่อยอดจากงานวิจัยและสิ่งประดิษฐ์สู่เชิงพาณิชย์ 2) สำรวจ ศึกษา วิเคราะห์ และประเมินทางวิชาการ รวมทั้งความต้องการพัฒนานวัตกรรม ในด้านต่าง ๆ เพื่อเสนอแนะนโยบายและมาตรการเกี่ยวกับการพัฒนานวัตกรรมของประเทศต่อคณะรัฐมนตรี 3) ส่งเสริมและสนับสนุนการยกระดับความสามารถด้านนวัตกรรมของเครือข่ายวิสาหกิจ ในสาขาอุตสาหกรรมยุทธศาสตร์ อันก่อให้เกิดระบบนวัตกรรมแห่งชาติที่เข้มแข็ง 4) ส่งเสริมและสนับสนุนการยกระดับทักษะความสามารถด้านเทคโนโลยีและการบริหารจัดการด้านนวัตกรรม 5) ส่งเสริมและสนับสนุนเพื่อสร้างความตื่นตัวด้านนวัตกรรมและเทคโนโลยีอันก่อให้เกิด วัฒนธรรมนวัตกรรม ทั้งในระดับผู้ประกอบการอุตสาหกรรม ระดับองค์กรและระดับประชาชน ซึ่งทั้ง 5 ประเด็นหลักในการขับเคลื่อนสำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) นี้ ล้วนแล้วแต่ต้องอาศัยข้อมูลในการขับเคลื่อนเป็นสำคัญ ทำให้ต้องบริหารจัดการด้านข้อมูลให้มีประสิทธิภาพ ตั้งแต่การนำเข้าข้อมูล การประมวลผลข้อมูล การใช้ข้อมูล รวมถึงการประเมินคุณภาพของข้อมูล ซึ่งต้องพิจารณาร่วมกับกฎระเบียบ นโยบาย มาตรฐาน ในการจัดทำนโยบายและแนวปฏิบัติด้านธรรมาภิบาลข้อมูลของกรม เพื่อที่จะทำให้สำนักงานสามารถดำเนินงานให้สอดคล้องกับวิสัยทัศน์ของสำนักงานต่อไป

2.2 การปฏิบัติ (Do)

สำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) ได้กำหนดพันธกิจที่จะต้องดำเนินการหลัก ๆ ได้แก่ ส่งเสริมการสร้างระบบนวัตกรรมแห่งชาติ สร้างโอกาสในการเข้าถึงและใช้ประโยชน์โครงสร้างพื้นฐานทางนวัตกรรม และยกระดับทักษะและความสามารถทางนวัตกรรมของกลุ่มเป้าหมาย ดังนั้นในการปฏิบัติต่าง ๆ ของกระบวนการธรรมาภิบาลข้อมูลจึงต้องดำเนินการให้สอดคล้อง จากผู้เกี่ยวข้องต่าง ๆ ได้แก่ คณะกรรมการ ผู้บริหาร เจ้าหน้าที่ของสำนักงาน และผู้ใช้บริการ ซึ่งต้องดำเนินการให้สอดคล้องกับกฎระเบียบ นโยบาย มาตรฐานและแนวปฏิบัติที่ได้กำหนดไว้ตามแผน ขณะที่คณะบริกรข้อมูลด้านธุรกิจ และด้านเทคนิคจะให้ความรู้และสนับสนุนให้บุคคลที่เกี่ยวข้องสามารถปฏิบัติตามกฎระเบียบเหล่านั้น รวมทั้งรายงานความก้าวหน้าผลการปฏิบัติงาน และประเด็นปัญหาที่พบระหว่างปฏิบัติงานจะถูกรายงานไปยังคณะกรรมการธรรมาภิบาลข้อมูลต่อไป

2.3 การตรวจสอบ วัดผล และรายงาน (Check, Measure and Report)

ในการตรวจสอบ คณะบริกรข้อมูลด้านคุณภาพจะดำเนินการตรวจสอบความสอดคล้องกันระหว่างกฎระเบียบนโยบาย และมาตรฐานที่กำหนด กับการปฏิบัติงานของบุคคลที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและผู้ที่เกี่ยวข้องอื่น ๆ พร้อมทั้งทำการวัดผลด้านคุณภาพข้อมูล ในส่วนของธรรมาภิบาลข้อมูล เรื่องคุณภาพข้อมูล ความมั่นคงปลอดภัย และความเสี่ยงต่าง ๆ ถือเป็นเรื่องสำคัญของการจัดการข้อมูล ก็จะต้องมีกระบวนการรายงานสิ่งต่าง ๆ ที่เกี่ยวข้องไปยังคณะกรรมการธรรมาภิบาลข้อมูลและผู้ที่เกี่ยวข้อง เพื่อให้ทราบถึงผลการดำเนินงานและประเด็นปัญหาที่พบในช่วงระยะเวลาที่เหมาะสมอย่างสม่ำเสมอ

2.4 การปรับปรุงอย่างต่อเนื่อง (Continual Improvement)

ธรรมาภิบาลข้อมูลเป็นสิ่งที่ต้องดำเนินการอย่างต่อเนื่องตลอดระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล ทั้งนี้สภาพแวดล้อมหรือกฎหมายที่เปลี่ยนแปลง รายการความต้องการจากผู้บริหารและผู้มีส่วนได้เสีย รวมถึงรายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัย รายงานความเสี่ยงต่อข้อมูล ควรจะต้องถูกใช้สำหรับการปรับปรุงกระบวนการธรรมาภิบาลข้อมูล นโยบาย กฎ ระเบียบ ข้อบังคับที่เกี่ยวข้องกับข้อมูล

เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูล เกณฑ์การวัดระดับคุณภาพข้อมูล และโครงสร้างธรรมาภิบาลข้อมูล โดยสามารถดำเนินการด้วยบุคลากรที่เกี่ยวข้องตามหน้าที่ที่รับผิดชอบ โดยมีความสัมพันธ์ระหว่างกระบวนการ/กิจกรรม ส่วนนำเข้า ผลลัพธ์ที่ต้องการ และผู้มีส่วนได้เสีย ดังนี้

กระบวนการ (Processes)	**ส่วนนำเข้า (Input)**	**ส่วนนำออก (Output)**	**ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholder)**
1 การวางแผน	(1) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมายที่เกี่ยวข้องกับข้อมูล (2) รายการชุดข้อมูล (3) รายการประเด็นปัญหาจากรายงานผลการตรวจสอบความสอดคล้องของการดำเนินงานต่อนโยบายข้อมูล รายงานคุณภาพข้อมูล รายงานความมั่นคงปลอดภัยต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล	(1) แผนดำเนินการ เช่น ขอบเขต เวลา กลุ่มธรรมาภิบาลข้อมูล และต้นทุน	(1) ผู้บริหารข้อมูลระดับสูง หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (2) คณะกรรมการธรรมาภิบาลข้อมูล (3) บริกรข้อมูลด้านธุรกิจ (4) บริกรข้อมูลด้านเทคนิค (5) บริกรข้อมูลด้านคุณภาพ
2 การปฏิบัติ	(1) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมายที่เกี่ยวข้องกับข้อมูล (2) แผนดำเนินการ (ขอบเขต เวลา และต้นทุน)	(1) รายงานความก้าวหน้าในการปฏิบัติงาน (2) ผลการปฏิบัติงาน (3) ประเด็นปัญหาที่พบระหว่างปฏิบัติงาน	(1) ผู้บริหารงาน (2) ผู้ปฏิบัติงานที่เกี่ยวข้อง (3) บริกรข้อมูลด้านธุรกิจ (4) บริกรข้อมูลด้านเทคนิค (5) บริกรข้อมูลด้านคุณภาพ
3 การตรวจสอบ วัดผล และรายงาน	(1) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมายที่เกี่ยวข้องกับข้อมูล (2) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูล ระดับคุณภาพข้อมูล	(1) รายงานผลการตรวจสอบความสอดคล้องของการดาเนินงานต่อนโยบาย ข้อมูล (2) รายงานคุณภาพข้อมูล รายงานความ มั่นคงปลอดภัยต่อข้อมูล และรายงาน ความเสี่ยงต่อข้อมูล	(1) บริกรข้อมูลด้านธุรกิจ (2) บริกรข้อมูลด้านเทคนิค (3) บริกรข้อมูลด้านคุณภาพ
4 การปรับปรุงธรรมาภิบาล	(1) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมายที่เกี่ยวข้องกับข้อมูล (2) โครงสร้างธรรมาภิบาลข้อมูล (3) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูล และระดับ คุณภาพข้อมูล (4) รายงานผลการตรวจสอบความสอดคล้องของการดาเนินงานต่อนโยบายข้อมูล รายงานความมั่นคงปลอดภัย	(1) กระบวนการธรรมาภิบาลข้อมูล (2) นโยบาย กฎ ระเบียบ ข้อบังคับและกฎหมาย ที่เกี่ยวข้องกับข้อมูล (3) เกณฑ์การประเมินความพร้อมของธรรมาภิบาลข้อมูลและระดับคุณภาพข้อมูล (4) โครงสร้างธรรมาภิบาลข้อมูล	(1) ผู้บริหารข้อมูลระดับสูงหรือผู้บริหาร เทคโนโลยีสารสนเทศระดับสูง (2) คณะกรรมการธรรมาภิบาลข้อมูล (3) บริกรข้อมูลด้านธุรกิจ (4) บริกรข้อมูลด้านเทคนิค (5) บริกรข้อมูลด้านคุณภาพ

กระบวนการ (Processes)	ส่วนนำเข้า (Input)	ส่วนนำออก (Output)	ผู้มีส่วนได้เสียกับข้อมูล (Data Stakeholder)
	ต่อข้อมูล และรายงานความเสี่ยงต่อข้อมูล (5) รายการความต้องการจากผู้บริหารและผู้มีส่วนได้เสีย		

3. มาตรการควบคุม (Controls)

เป็นมาตรการที่กำหนดขึ้นมาเพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย และไม่ถูกละเมิดความเป็นส่วนบุคคล รวมทั้งสามารถเชื่อมโยง แลกเปลี่ยน บูรณาการ และใช้ประโยชน์ได้อย่างมีประสิทธิภาพ ดังนี้

3.1 การบริหารจัดการข้อมูล (Data Management)

การบริหารจัดการข้อมูล หมายถึง ขั้นตอนการสร้างข้อมูล การรวบรวมข้อมูล การจัดเก็บ การจัดเก็บถาวร การทำลายข้อมูล การประมวลผลข้อมูล การใช้ข้อมูล การแลกเปลี่ยน การเชื่อมโยงข้อมูล และการเปิดเผยข้อมูลต่อสาธารณะ

การบริหารจัดการข้อมูลเป็นสิ่งสำคัญสำหรับทุกหน่วยงาน ซึ่งกรมพัฒนาธุรกิจการค้าตระหนักว่าข้อมูลที่มีอยู่เป็นทรัพย์สินที่มีค่า และจากการเกิดขึ้นของข้อมูลที่มีปริมาณมหาศาล ไม่ว่าจะเป็นข้อมูลที่รวบรวมมาโดยอัตโนมัติจากระบบหรืออุปกรณ์ต่าง ๆ หรือข้อมูลที่เกิดขึ้นจากการป้อนข้อมูลหรือโต้ตอบกับผู้ใช้งาน เพื่อให้กรมสามารถนำข้อมูลเหล่านี้ไปประมวลผลหรือใช้ในการตัดสินใจได้อย่างแม่นยำ จึงต้องได้รับการบริหารจัดการอย่างถูกต้อง เหมาะสม และสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของหน่วยงาน เช่น

1) เพื่อการจัดเก็บ นำมาใช้งาน และประมวลผลข้อมูลตามที่หน่วยงานต้องการ
2) เพื่อควบคุม ตรวจสอบ และป้องกัน โดยใช้กระบวนการธรรมาภิบาลข้อมูลและความปลอดภัยของข้อมูล
3) เพื่อจัดหมวดหมู่ และกำหนดมาตรฐานของข้อมูล โดยใช้การจำแนกข้อมูล และกำหนดกรอบการทำงานที่เป็นที่รู้จักแพร่หลาย
4) เพื่อให้สามารถนำข้อมูลกลับมาใช้ได้ในภายหลัง โดยกำหนดข้อมูลให้อยู่ในรูปแบบที่เรียกใช้ได้อย่างมีประสิทธิภาพ
5) เพื่อการปรับปรุงข้อมูลให้เป็นปัจจุบัน และมีความถูกต้องสมบูรณ์อยู่เสมอ
6) เพื่อการปกป้องข้อมูลจากการลักลอบใช้งานหรือแก้ไขโดยมิชอบ รวมถึงจากเหตุการณ์ที่อาจเกิดจากภัยธรรมชาติหรือความบกพร่องภายในระบบคอมพิวเตอร์ ซึ่งในการบริหารจัดการข้อมูลนั้นมีองค์ประกอบในการบริหารจัดการตลอดทั้งระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล

ระบบบริหารและกระบวนการจัดการข้อมูล หรือวงจรชีวิตของข้อมูล คือ “ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล” ประกอบด้วย 6 ขั้นตอน ดังนี้

1) กระบวนการสร้างข้อมูล (Create) เป็นการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เช่น อุปกรณ์ตรวจจับสัญญาณ (Sensor) รวมถึงการซื้อข้อมูล หรือการรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บในภายหลัง โดยการดำเนินการเป็นไปตามบทบัญญัติของกฎหมาย และระเบียบที่เกี่ยวข้อง ดังนี้

1.1) มีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

1.2) เจ้าของข้อมูล และบริกรข้อมูล เป็นผู้ร่วมกันจัดให้มีชุดข้อมูลและเมทาดาตาที่มีความถูกต้องครบถ้วน และเป็นปัจจุบัน

1.3) เจ้าของข้อมูล ต้องจัดชั้นความลับของข้อมูล

2) กระบวนการจัดเก็บข้อมูล (Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้าง หรือข้อมูลที่ได้จากการแลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลาย และให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว ไม่ว่าจะจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS) โดยดำเนินการเป็นไปตามบทบัญญัติของกฎหมาย และระเบียบที่เกี่ยวข้อง ดังนี้

2.1) มีการดำเนินการโดยบุคลากรของสำนักงานซึ่งมีหน้าที่รับผิดชอบการดำเนินการนั้น

2.2) มีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

2.3) การจัดเก็บข้อมูล ทำโดยจัดเก็บลงในสื่อบันทึกข้อมูลและมีโครงสร้างข้อมูล ข้อมูลหลักและข้อมูลอ้างอิงตามที่สำนักงานกำหนด

2.4) การจัดเก็บข้อมูล มีการสำรองข้อมูลที่จัดเก็บ ให้มีความถูกต้องครบถ้วนและเป็นปัจจุบัน โดยมีการสำรองข้อมูลที่ทำให้มั่นใจได้ว่าข้อมูลจะไม่สูญหายยกเว้นกรณีสุดวิสัย

2.5) ในกรณีที่การดำเนินการจัดเก็บข้อมูล ส่งผลต่อชุดข้อมูลและเมทาดาตา เจ้าของข้อมูลและบริกรข้อมูลต้องดำเนินการปรับปรุงชุดข้อมูลและเมทาดาตาให้มีความถูกต้อง ครบถ้วนและเป็นปัจจุบัน

3) กระบวนการใช้ข้อมูล (Use) เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้

เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore) โดยดำเนินการเป็นไปตามบทบัญญัติของกฎหมาย และระเบียบที่เกี่ยวข้อง ดังนี้

3.1) ให้มีการดำเนินการโดยบุคลากรของกรมซึ่งมีหน้าที่รับผิดชอบการดำเนินการนั้น

3.2) มีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

3.3) ข้อมูลมีความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความต้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) และมีความพร้อมใช้ (Availability) มีการบันทึกประวัติการใช้ (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

4) กระบวนการเผยแพร่ข้อมูล (Publish) เป็นการแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition) โดยดำเนินการโดยบุคลากรของกรมซึ่งมีหน้าที่รับผิดชอบการดำเนินการนั้น โดยให้เป็นไปตามบทบัญญัติของกฎหมาย และระเบียบที่เกี่ยวข้อง

5) กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการคัดลอกเอาข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อทำสำเนาสำหรับการเก็บรักษา โดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ โดยดำเนินการเป็นไปตามบทบัญญัติของกฎหมาย และระเบียบที่เกี่ยวข้อง ดังนี้

5.1) มีการดำเนินการโดยบุคลากรของกรมซึ่งมีหน้าที่รับผิดชอบการดำเนินการนั้น

5.2) มีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

5.3) การจัดเก็บถาวร เป็นการดำเนินการกับข้อมูลที่ไม่มีการลบ ปรับปรุงหรือแก้ไขอีกต่อไป และสามารถนำกลับมาใช้งานได้ใหม่เมื่อต้องการ

5.4) ในกรณีที่การดำเนินการจัดเก็บข้อมูลส่งผลต่อชุดข้อมูลและเมทาดาตา เจ้าของข้อมูลและบริกรข้อมูลต้องดำเนินการปรับปรุงชุดข้อมูลและเมทาดาตาให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

6) กระบวนการทำลายข้อมูล (Destroy) เป็นการทำลายข้อมูล ซึ่งปกติจะเป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด โดยดำเนินการเป็นไปตามบทบัญญัติของกฎหมาย และระเบียบที่เกี่ยวข้อง ดังนี้

6.1) มีการดำเนินการโดยบุคลากรของกรมซึ่งมีหน้าที่รับผิดชอบการดำเนินการนั้น

6.2) มีการรักษาความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

6.3) การทำลายข้อมูล เป็นการดำเนินการกับข้อมูลที่ไม่ต้องการนำกลับมาใช้งานได้อีกต่อไป

6.4) ในกรณีที่การทำลายข้อมูล ส่งผลต่อชุดข้อมูลและเมทาดาตา เจ้าของข้อมูล และบริกรข้อมูลต้องดำเนินการปรับปรุงชุดข้อมูลและเมทาดาตาให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

3.2 ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy)

ความมั่นคงปลอดภัยของข้อมูล (Data Security) หมายความว่า การป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล สอดคล้องกับข้อมูลของมาตรฐาน ISO/IEC27001 โดยมีรายละเอียด ดังนี้

1) **การรักษาความลับ (Confidentiality)** หมายความว่าการรักษาปลอดภัยของข้อมูลตามระดับชั้น ของข้อมูล และมีการกำหนดสิทธิ์การเข้าถึงข้อมูลนั้น เนื่องจากข้อมูลในหน่วยงานอาจมีหลายประเภท ข้อมูลบางประเภทเป็นข้อมูลที่มีความสำคัญ หรืออ่อนไหว จึงต้องมีการรักษาความลับเพื่อลดความเสี่ยงของ การถูกคุกคาม และเป็นการป้องกันการรั่วไหลของข้อมูลโดยมิชอบ เช่น การส่งข้อมูลที่ปกปิดหรือเป็นความลับ ต้องมีวิธีการที่ทำให้ทราบได้ว่าบุคคลที่ต้องการส่งข้อมูลมาให้ หรือการที่ผู้ได้รับการอนุญาตให้เข้าถึงข้อมูล เท่านั้นทีสามารถอ่านข้อมูลได้
2) **ความถูกต้องของข้อมูล (Integrity)** หมายความว่าการคงสภาพของข้อมูลหรือการรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความถูกต้องและน่าเชื่อถือ รวมถึงมีการปกป้องข้อมูลให้ปราศจากการถูก เปลี่ยนแปลงโดยผู้ไม่มีสิทธิ์ เช่น ข้อมูลที่ใช้จะต้องเป็นข้อมูลที่ถูกต้องอย่างแท้จริง ไม่มีการดัดแปลงหรือแก้ไข ระหว่างทาง
3) **ความพร้อมใช้งานของข้อมูล (Availability**) หมายความว่าการพร้อมในการใช้งานอยู่เสมอ กล่าวคือ ข้อมูลต้องพร้อมสำหรับการใช้งานได้เสมอ รวมถึงมีการสำรองข้อมูลไว้เมื่อเกิดภัยพิบัติหรือเหตุการณ์ ที่ไม่คาดฝัน เช่น หากต้องการใช้ข้อมูล ผู้ใช้งานสามารถใช้ข้อมูลได้ทันที และใช้ได้อย่างต่อเนื่อง

โดยความมั่นคงปลอดภัยของข้อมูลต้องดำเนินการตั้งแต่การวางแผน การจัดทำ การปฏิบัติตาม และการบังคับใช้นโยบายและขั้นตอนด้านการรักษาความปลอดภัย เพื่อสนับสนุนในด้านที่เกี่ยวข้องกับการพิสูจน์ตัวตน การกำหนดสิทธิ์ การเข้าถึงข้อมูล การตรวจสอบ และความพร้อมใช้ของข้อมูลอย่างเหมาะสม

นอกจากนี้ ต้องมีการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy) ตั้งแต่การรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูล โดยจะต้องมีการระบุวัตถุประสงค์เป็นหลักฐานให้ชัดเจน ห้ามมิให้มีการเปิดเผย หรือแสดง หรือทำให้ปรากฏในลักษณะอื่นใดที่ไม่สอดคล้องกับวัตถุประสงค์ เว้นแต่จะ ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้น ๆ หรือมีกฎหมายกำหนดให้สามารถกระทำสิ่งนั้นได้

3.3 คุณภาพของข้อมูล (Data Quality)

คุณภาพของข้อมูล (Data Quality) เป็นเครื่องมือในการวัดความน่าเชื่อถือและประสิทธิภาพของการนำข้อมูลไปใช้ ต้องมีการวางแผน การดำเนินการ และการควบคุมกิจกรรมต่าง ๆ รวมถึงการปรับปรุง เพื่อให้ข้อมูลมีคุณภาพ เนื่องจากข้อมูลที่มีคุณภาพสูงทำให้การดำเนินงานของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ การทำให้ข้อมูลมีคุณภาพ ประกอบด้วย

1) ความถูกต้องและสมบูรณ์ (Accuracy and Completeness)
2) ความสอดคล้องกัน (Consistency)
3) ตรงตามความต้องการของผู้ใช้ (Relevancy)
4) ความเป็นปัจจุบัน (Timeliness)
5) ความพร้อมใช้ (Availability)

ดังแสดงรายละเอียดเพิ่มเติมในบทที่ 4.1 การประเมิน คุณภาพของข้อมูล (Data Quality Assessment)

3.4 มาตรการควบคุม

เป็นมาตรการที่กำหนดขึ้นมาเพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัยและไม่ถูกละเมิดความเป็นส่วนบุคคล รวมทั้งสามารถเชื่อมโยง แลกเปลี่ยน บูรณาการ และใช้ประโยชน์ได้อย่างมีประสิทธิภาพ ปัจจุบันกฎหมายที่เกี่ยวข้องกับข้อมูล ข่าวสาร หรือสิทธิส่วนบุคคลในประเทศไทย มีประเด็นที่อาจส่งผลกระทบต่อหลักแนวคิดธรรมาภิบาลข้อมูล ซึ่งหากหน่วยงานในประเทศไทยต้องการสร้างหรือปรับปรุงระบบภายในให้มีธรรมาภิบาลข้อมูล จะต้องพิจารณาประเด็นหลัก ๆ ที่เกี่ยวข้องกับกฎหมาย

1) การเปิดเผยข้อมูล

การเปิดเผยข้อมูลเป็นสิ่งจำเป็นต่อการดำเนินงานของกรมพัฒนาธุรกิจการค้า ซึ่งแสดงความโปร่งใส ในการดำเนินงานและความสามารถในการตรวจสอบได้จากภาคเอกชนและประชาชน รวมไปถึงการสนับสนุนให้ภาคเอกชนและประชาชนนำข้อมูลที่เปิดเผยไปสร้างนวัตกรรมผลิตภัณฑ์และบริการเพื่อยกระดับการพัฒนาประเทศ โดยแนวคิดการเปิดเผยข้อมูลเป็นที่ยอมรับของหน่วยงานระหว่างประเทศและรัฐบาลประเทศต่างๆ ซึ่งดำเนินการตามแนวปฏิบัติและมาตรฐานเชิงเทคนิคจากส่วนกลาง เพื่อให้หน่วยงานภาครัฐนำไปใช้เป็นแนวปฏิบัติในการดำเนินการเกี่ยวกับการเปิดเผยข้อมูลของหน่วยงานให้เป็นไปในทิศทางเดียวกัน

2) การเชื่อมโยงและแลกเปลี่ยนข้อมูล

การเชื่อมโยงและแลกเปลี่ยนข้อมูลเป็นสิ่งสำคัญต่อการบูรณาการการดำเนินงานระหว่างหน่วยงานภาครัฐ ซึ่งเป็นประโยชน์ต่อหน่วยงานภาครัฐและประชาชนในการขอใช้บริการจากภาครัฐ โดยสำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) ได้ดำเนินการให้สอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 โดยมีการพัฒนามาตรฐาน หลักเกณฑ์ และวิธีการเกี่ยวกับดิจิทัล และพัฒนาโครงสร้างพื้นฐานด้านดิจิทัลที่จำเป็น ให้เป็นไปตามมาตรฐานสากล เพื่อสร้างและพัฒนากระบวนการทำงานของหน่วยงานของรัฐให้มีความสอดคล้องและมีการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกัน รวมทั้งมีความมั่นคงปลอดภัยและน่าเชื่อถือโดยมีการบูรณาการและสามารถทำงานร่วมกันอย่างเป็นเอกภาพ เกิดการ

พัฒนาการบริการภาครัฐ ที่มีประสิทธิภาพและนำไปสู่การบริหารราชการและการบริการประชาชนแบบบูรณาการ รวมทั้งให้ประชาชนเข้าถึงโดยสะดวก

3) การคุ้มครองข้อมูลส่วนบุคคล

การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) เป็นสิ่งสำคัญที่ภาครัฐต้องดำเนินการ โดยปัจจุบันมีการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทาง อิเล็กทรอนิกส์อย่างแพร่หลาย ซึ่งหน่วยงานภาครัฐอาจจะมีการเก็บ รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลของ ผู้ใช้บริการในรูปของข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการป้องกันการละเมิดข้อมูลส่วนบุคคล ซึ่งเป็นสิทธิขั้นพื้นฐาน สำคัญในความเป็นส่วนบุคคล (Privacy Right) ของประชาชนที่ต้องได้รับการคุ้มครอง อันจะทำให้ประชาชนมี ความมั่นใจในการทำธุรกรรมทางอิเล็กทรอนิกส์ ดังนั้นการคุ้มครองข้อมูลส่วนบุคคลจำเป็นที่จะต้องนำมา วิเคราะห์เพื่อให้เกิดธรรมาภิบาลข้อมูลภาครัฐที่ดี โดยมีกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

3.1) พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540 กำหนดประเภทข้อมูลที่เปิดเผยได้และเปิดเผยไม่ได้ ซึ่งเป็นสิ่งที่จำเป็นต้องมีการพิจารณาในกรณีที่เป็นข้อมูลส่วนบุคคล เนื่องจากข้อมูลที่เป็น ข้อมูลส่วนบุคคลจำเป็นต้องได้รับการคุ้มครองอย่างมีหลักเกณฑ์

3.2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้มีการกำหนดหลักเกณฑ์ กลไก และมาตรการที่กำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคล

4) การรักษาความลับ

การรักษาความลับทางราชการเป็นสิ่งที่จำเป็นต่อการดำเนินงานของหน่วยงานภาครัฐ ซึ่งเป็นการป้องกนความเสียหายที่จะเกิดขึ้นต่อภาครัฐ ทั้งในด้านชื่อเสียง การเงิน ความสามารถในการพัฒนาประเทศ และความมั่นคงของประเทศ ดังนั้นทุกชุดข้อมูลต้องมีการจัดลำดับชั้นความลับของข้อมูลดังต่อไปนี้

4.1) ระดับที่ 1: ข้อมูลสาธารณะ ได้แก่ ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ

4.2) ระดับที่ 2: ข้อมูลส่วนบุคคล ได้แก่ ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล ที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้น ๆ ได้ทั้งทางตรงหรือทางอ้อม

4.3) ระดับที่ 3: ข้อมูลความลับทางราชการ ได้แก่ ข้อมูลที่อยู่ในความครอบครอง หรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย

4.4) ระดับที่ 4: ข้อมูลความมั่นคง ได้แก่ ข้อมูลเกี่ยวกับความมั่นคงของรัฐ ที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น

โดยมีกฎหมาย ระเบียบที่เกี่ยวข้องกับการรักษาความลับ อาทิ พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ.๒๕๖๒ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติมได้มีข้อกำหนดที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล ได้แก่ กำหนดนิยามข้อมูลข่าวสารลับ และกำหนดหลักเกณฑ์และวิธีการในการรักษาความลับของหน่วยงานภาครัฐ

เพื่อให้การบริหารจัดการ บูรณาการข้อมูลและการปฏิบัติงาน มีความสอดคล้องและเชื่อมโยงเข้าด้วยกัน รวมทั้งเพิ่มประสิทธิภาพในการอำนวยความสะดวกการให้บริการ สามารถเข้าถึงประชาชน สำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) จึงได้มีการอนุญาตให้เข้าถึงข้อมูลต่าง ๆ ซึ่งอาจเป็นช่องโหว่ที่มีความเสี่ยงในการถูกโจมตี หรือการเจาะระบบได้ โดยได้กำหนดมาตรการการให้บริการอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล ตามประกาศสำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) เรื่อง แนวนโยบายและแนวปฏิบัติใน

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2561 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 อย่างสม่ำเสมอ

4. การวัดผลการบริหารจัดการข้อมูล (Data Management Measurements)

การวัดการดำเนินการธรรมาภิบาลข้อมูล เป็นการประเมินความพร้อมของธรรมาภิบาลข้อมูลจะแสดงให้เห็นถึงสถานะปัจจุบันของกรมพัฒนาธุรกิจการค้า ในเรื่องความพร้อมและความก้าวหน้า ในการดำเนินการธรรมาภิบาลข้อมูล ซึ่งผลของการดำเนินการธรรมาภิบาลข้อมูลจะส่งผลถึงความสำเร็จของธรรมาภิบาลข้อมูลที่ประกอบด้วย คุณภาพของข้อมูล ความมั่นคงปลอดภัยของข้อมูล และมูลค่าเชิงธุรกิจโดยมีแนวทางการประเมินความพร้อม การประเมินคุณภาพของข้อมูล และการประเมินความมั่นคงปลอดภัยของข้อมูล ดังนี้

4.1 **การประเมินความพร้อมของธรรมาภิบาลข้อมูล (Data Governance Readiness Assessment)**

ระดับความพร้อมของธรรมาภิบาลข้อมูลกรมพัฒนาธุรกิจการค้า จะถูกใช้เป็นเครื่องมือในการประเมินความพร้อมของธรรมาภิบาลข้อมูลซึ่งประกอบด้วย 6 ระดับ ตั้งแต่ 0 - 5 โดยพิจารณาถึงการดำเนินการให้มีในแต่ละส่วนประกอบด้วย โครงสร้างธรรมาภิบาลข้อมูล กระบวนการธรรมาภิบาลข้อมูล นโยบายข้อมูลและการตรวจสอบ การประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย และกระบวนการปรับปรุงอย่างต่อเนื่อง โดยกำหนดรายละเอียดความพร้อมของหน่วยงาน ออกเป็นแต่ละระดับดังนี้

2) ระดับ 0: None หมายถึง ไม่มีธรรมาภิบาลข้อมูล หรือมีแต่ไม่ได้ดำเนินการอย่างเป็นทางการ
3) ระดับ 1: Initial หมายถึง มีการเริ่มดำเนินการ แต่ยังไม่มีการกำหนดมาตรฐานของกระบวนการ
4) ระดับ 2: Managed หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงาน
5) ระดับ 3: Standardized หมายถึง มีกระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำกับและติดตามข้อมูล มีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน
6) ระดับ 4: Advanced หมายถึง มีกระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำกับและติดตามข้อมูล มีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตามวิเคราะห์ และรายงานคุณภาพข้อมูลและความมั่นคงปลอดภัย
7) ระดับ 5: Optimized หมายถึง มีการดำเนินการสอดคล้องกับระดับ 4 รวมทั้งมีการวิเคราะห์สาเหตุของปัญหา และการปรับปรุงกระบวนการอย่างต่อเนื่อง

จะเห็นได้ว่าในแต่ละระดับนั้น มีการเพิ่มกระบวนการมากขึ้นเรื่อย ๆ เพื่อให้กระบวนการธรรมาภิบาลข้อมูลมีความสมบูรณ์ ในลักษณะของ PDCA (plan-do-check-act) ที่เป็นวงรอบปิด โดยเริ่มตั้งแต่กระบวนการถูกกำหนดเป็นแผนงาน ออกมาตรฐานของหน่วยงาน มีการกำกับและติดตามข้อมูล มีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลและความมั่นคงปลอดภัย มีการวิเคราะห์สาเหตุของปัญหา และการปรับปรุงกระบวนการอย่างต่อเนื่อง

4.2 **การประเมินคุณภาพของข้อมูล (Data Quality Assessment)**

การประเมินคุณภาพของข้อมูล เพื่อตรวจสอบผลลัพธ์ หรือความสำเร็จจากธรรมาภิบาลข้อมูลของสำนักงานนวัตกรรมแห่งชาติ (องค์การมหาชน) โดยองค์ประกอบในการประเมินคุณภาพ ดังนี้

1) **ความถูกต้อง และสมบูรณ์ (Accuracy and Completeness)** หมายความว่า ข้อมูลมีความถูกต้องแม่นยำสูง มีความครบถ้วนสมบูรณ์ของข้อมูลที่เก็บรวบรวมมา และมีการตรวจสอบความถูกต้องระหว่างข้อมูลในส่วนต่าง ๆ ในทุกขั้นตอน เพื่อให้ข้อมูลถูกต้องเชื่อถือได้และให้ผลลัพธ์ตรงตามความต้องการผู้ใช้ (ข้อมูลครบถ้วน ข้อมูลไม่ขาดหาย กว้างพอและลึกพอสำหรับการใช้งาน)
2) **ข้อมูลมีความต้องกัน (Consistency)** หมายความว่า ข้อมูลมีความสอดคล้องกันของแนวคิด คำนิยาม วิธีการ รหัส และการนำเสนอที่ทำให้ข้อมูลจากต่างแหล่ง ต่างเวลา สามารถเปรียบเทียบข้ามช่วงเวลาและบูรณาการข้อมูลเพื่อใช้ประโยชน์ร่วมกันได้
3) **ความเป็นปัจจุบัน (Timeliness)** หมายความว่า ข้อมูลเป็นปัจจุบันทันสมัยเพียงพอต่อการใช้งานและพร้อมใช้งานตามที่กำหนดและในกรอบเวลาที่กำหนดไว้ หรือมีข้อมูลทันต่อการใช้งานทุกครั้งตามที่ผู้ใช้ต้องการ
4) **ตรงตามความต้องการของผู้ใช้ (Relevancy)** หมายความว่า ข้อมูลสามารถนำไปใช้ได้กับงานที่ทำอยู่ เป็นข้อมูลที่ผู้ใช้งานต้องการ หรือเป็นข้อมูลที่จำเป็นต้องทราบ มีมุมมองและความละเอียดเพียงพอต่อการนำไปใช้งาน
5) **ความพร้อมใช้ (Availability)** หมายความว่า ข้อมูลเข้าถึงได้ง่าย หรือมีข้อมูลนั้นอยู่สามารถใช้งานได้จริง และสามารถใช้งานได้ตลอดเวลา

4.3 **การประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security Assessment)**

การประเมินความมั่นคงปลอดภัยของข้อมูลเป็นอีกหนึ่งวิธีในการวัดความสำเร็จจากธรรมาภิบาลข้อมูล โดยใช้หลักเกณฑ์ในด้านต่าง ๆ ดังนี้

1) จัดทำนโยบายด้านความมั่นคงปลอดภัยของข้อมูลที่รวมถึงการป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล
2) ข้อมูลมีการจัดชั้นความลับ (Data Classification) ข้อมูลควรมีการจัดชั้นความลับให้สอดคล้องกับกฎหมาย เงื่อนไข และข้อกำหนดต่าง ๆ รวมถึงการคำนึงถึงมูลค่า ความสำคัญ และความอ่อนไหวของข้อมูลกรณีที่ผู้ไม่ได้รับสิทธิในการเข้าถึงนั้นทำการเปิดเผยข้อมูลดังกล่าวด้วย การกำหนดระดับชั้นความลับ เช่น ข้อมูลลับ ข้อมูลลับมาก และข้อมูลเปิดเผยได้
3) กำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูล (Data Protection) การกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลต้องคำนึงถึงระดับชั้นความลับของข้อมูล เช่น ข้อมูลที่มี

ความอ่อนไหวต้องมีการกำหนดมาตรการควบคุมและป้องกันการเข้าถึงข้อมูลแบบพิเศษ เพื่อป้องกันการเข้าถึงเพื่อเปิดเผยข้อมูลที่อ่อนไหวนั้น รวมถึงเพื่อป้องกันการดัดแปลง แก้ไข แต่งเติมข้อมูลโดยไม่ได้รับอนุญาต

4) ข้อมูลถูกใช้งานอย่างเหมาะสม การนำข้อมูลไปใช้ควรดำเนินการให้สอดคล้องกับสัญญาอนุญาตและไม่ขัดต่อกฎหมาย

5) ข้อมูลต้องมีความพร้อมใช้อยู่เสมอ ต้องมีการดำเนินการเตรียมความพร้อมไม่ว่าข้อมูลจะอยู่ในประเภทใดก็ตาม เช่น ข้อมูลในรูปแบบกระดาษต้องมีสถานที่จัดเก็บดูแล และสามารถเข้าถึงโดยผู้มีสิทธิได้อย่างสม่ำเสมอ ข้อมูลในรูปแบบอิเล็กทรอนิกส์ต้องมีการเตรียมความพร้อมเรื่องระบบงาน การสำรองข้อมูลรวมถึงมีแผนการดำเนินการในกรณีฉุกเฉินใด ๆ ที่อาจมีผลต่อการใช้ข้อมูลด้วย

ในการวัดความมั่นคงปลอดภัยของข้อมูล สามารถคิดเป็นค่าดัชนีชี้วัดเป็นร้อยละโดยพิจารณาถึงจำนวนเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูล เช่น เหตุละเมิดการเผยแพร่ข้อมูลโดยไม่ได้รับอนุญาตจะคิดจากจำนวนที่ควบคุมได้กับจำนวนทั้งหมดที่เกิดขึ้น จำนวนข้อร้องเรียนต่าง ๆ จะคิดจากร้อยละ ของจำนวนข้อร้องเรียนด้านความมั่นคงปลอดภัยข้อมูลที่ลดลงโดยเทียบกับปีที่ผ่านมา ความสำเร็จในการกู้คืนข้อมูลจะคิดเทียบกับการจำนวนครั้งของการกู้คืนข้อมูลทั้งหมด

5. ข้อมูลและการจำแนกหมวดหมู่ของข้อมูล (Data and Data Categories)

5.1 ข้อมูล

1) คำนิยาม

1.1) **บัญชีข้อมูลภาครัฐ (Government Data Catalog)** หมายความว่า เอกสารแสดงบรรดารายการของ ชุดข้อมูลสำคัญที่รวบรวมจากบัญชีข้อมูลของหน่วยงานภาครัฐ

1.2) **ข้อมูลเปิดภาครัฐ (Open Data)** หมายความว่า ข้อมูลที่หน่วยงานของรัฐต้องเปิดเผยต่อสาธารณะ อย่างน้อยตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัลที่สามารถเข้าถึงและใช้ได้ อย่างเสรี ไม่จำกัดแพลตฟอร์ม ไม่เสียค่าใช้จ่าย เผยแพร่ ทำซ้ำหรือใช้ประโยชน์ได้โดยไม่จำกัดวัตถุประสงค์

1.3) **ข้อมูลหลัก (Master Data)** หมายความว่า ข้อมูลที่ถูกสร้างขึ้นเป็นข้อมูลพื้นฐานที่มีความสำคัญต่อ การ ดำเนินงาน เพื่อใช้งานร่วมกันภายในหน่วยงานเป็นหลักและขับเคลื่อนองค์กรให้บรรลุเป้าหมาย เช่น ข้อมูลระเบียนผู้ประกอบการนวัตกรรม ข้อมูลโครงการนวัตกรรม ข้อมูลทะเบียนสัญญาการับทุน ข้อมูลระเบียนวิสาหกิจเริ่มต้น ข้อมูลหลักสูตรฝึกอบรมด้านนวัตกรรม และข้อมูลสนับสนุนการพิสูจน์และยืนยันตัวตนของบุคคลและนิติบุคคล

1.4) **ข้อมูลอ้างอิง (Reference Data)** หมายความว่า ข้อมูลที่ถูกสร้างขึ้น หรืออ้างอิงมาจากข้อมูลหลัก เพื่อกำหนดให้เป็นมาตรฐานและใช้งานร่วมกันในวงกว้าง โดยมีการระบุแหล่งที่มาที่ใช้อ้างอิงได้ชัดเจน หรือ มี หน่วยงานรับผิดชอบเป็นทางการ เช่น ข้อมูลชื่อจังหวัด ข้อมูลรหัสไปรษณีย์

1.5) **ข้อมูลแบ่งปัน (Shared data)** หมายความว่า ข้อมูลอ่อนไหวที่ได้รับการจัดระดับชั้นข้อมูล ยกเว้นใน ระดับชั้นลับที่สุด ซึ่งสามารถแบ่งปันและแลกเปลี่ยนกันได้ระหว่าง

หน่วยงาน โดยจำเป็นต้องมีการกำหนดสิทธิ ในการเข้าถึงและใช้งาน รวมถึงการคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย

1.6) **ระดับชั้นข้อมูล (Data Classification Level)** หมายความว่า ระดับชั้นข้อมูลเพื่อจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจ โดยข้อมูลที่มีความอ่อนไหวแบ่งระดับชั้นออกเป็น ชั้นเปิดเผย (Open) ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) ชั้นลับมาก (Secret) และ ชั้นลับที่สุด (Top Secret) ซึ่งข้อมูลที่มีระดับชั้น ลับ (Confidential) ลับมาก (Secret) และ ลับที่สุด (Top Secret) เป็นเพียงการจัดระดับชั้นข้อมูล ไม่ใช่การกำหนดให้ข้อมูลนั้นเป็นข้อมูลความลับทางราชการตามระเบียบการรักษาความลับทางราชการ

2) **ประเภทของข้อมูล (Types of Data)** แบ่งออกได้เป็น 3 ประเภท ดังนี้

2.1) ข้อมูลที่มีโครงสร้าง (Structured Data) เป็นข้อมูลที่มีการนิยามโครงสร้างของข้อมูลไว้โดย นิยามความหมายและคุณสมบัติของแต่ละฟิลด์ข้อมูล โครงสร้างมีชั้นเดียวทำให้ง่ายต่อการค้นหา เช่น ตารางข้อมูลในฐานข้อมูล Comma-Separated Values – CSV

2.2) ข้อมูลกึ่งโครงสร้าง(Semi-structuredData)เป็นข้อมูลที่มีการนิยามโครงสร้างของข้อมูลไว้แต่ โครงสร้างเป็นแบบลำดับขั้น (Hierarchy) เช่น Extensible Markup Language - XML JavaScript Object Notation – JSON

2.3) ข้อมูลที่ไม่มีโครงสร้าง (Unstructured Data) เป็นข้อมูลที่ไม่ได้มีการนิยามโครงสร้างของข้อมูล ไว้ มักจะอยู่ในรูปแบบ เช่น ข้อความ รูปภาพ เสียง วีดิทัศน์

3) **ชุดข้อมูล (Datasets)** คือ การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของ ข้อมูล หรือจากการใช้ประโยชน์ของข้อมูล

5.2 การจำแนกหมวดหมู่ของข้อมูล (Data Categories)

เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิ เข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติ ตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่ การบริหารจัดการข้อมูลอย่างเป็นระบบ ซึ่งมีการแบ่งหมวดหมู่ของข้อมูลออกได้เป็น 5 หมวด ดังนี้

1) **ข้อมูลสาธารณะ (Public Data)** หมายความว่า ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่าง อิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น

2) **ข้อมูลใช้ภายใน (Internal Use Only)** หมายความว่า ข้อมูลสำหรับใช้ในการดำเนินกิจการภายใน ของหน่วยงานซึงไม่อนุญาตให้นำไปใช้งานภายนอกก่อนได้รับอนุญาตจากเจ้าของข้อมูล เช่น ร่างนโยบาย ร่าง มาตรฐาน และขั้นตอนการปฏิบัติงาน ประกาศ และบันทึกภายในหน่วยงานที่อยู่ระหว่างการขออนุมัติ เป็นต้น

3) **ข้อมูลส่วนบุคคล (Personal Data)** หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัว บุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม (หมายเหตุ ในกรณีที่ต้องดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคลตามวัตถุประสงค์ของกฎหมายจะไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ)

4) **ข้อมูลความลับทางราชการ (Classified Information)** หมายความว่า ข้อมูลข่าวสารตามมาตรา 14 หรือมาตรา 15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่มีคำสั่ง

ไม่ให้เปิดเผยและอยู่ ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐ หรือที่เกียวกับเอกชน ซึ่งมีการกำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือ ชั้นลับที่สุด ตามระเบียบว่า ด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม โดยคำนึงถึงการปฏิบัติหน้าที่ของ หน่วยงานของรัฐและประโยชน์แห่งรัฐประกอบกัน

5) **ข้อมูลความมั่นคง (National Security Information)** หมายความว่า ข้อมูลภายใต้กรอบความ มั่นคงแห่งชาติ หรือ ภาวะที่ประเทศปลอดจากภัยคุกคามต่อเอกราช อธิปไตยบูรณภาพแห่งอาณาเขต สถาบัน ศาสนา สถาบันพระมหากษัตริย์ ความปลอดภัยของประชาชน การดำรงชีวิต โดยปกติสุขของประชาชน หรือที่ กระทบต่อผลประโยชน์แห่งชาติหรือการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข รวมทั้งความพร้อมของประเทศที่จะเผชิญสถานการณ์ต่าง ๆ อันเกิดจากภัยคุกคามทุกรูปแบบ และครอบคลุม ด้านความมั่นคงปลอดภัยของประเทศ (National Security) ในมิติเศรษฐกิจ อาหาร สุขภาพ สิ่งแวดล้อมและสิทธิมนุษยชน ส่วนบุคคล ชุมชน การเมือง และการต่างประเทศ ที่สอดคล้องตามเป้าหมายของนโยบายและ แผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ