นโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูล

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

Department of Primary Industries and Mines (DPIM)

นโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูล

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

Department of Primary Industries and Mines (DPIM)

Data Policy and Data Governance Guidelines

เวอร์ชัน ๑.๐ | ปีงบประมาณ ๒๕๖๘

จัดทำโดย : ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทที่ ๑ บทนำและคำนิยาม

๑.๑ หลักการและเหตุผล

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ (กพร.) ในฐานะหน่วยงานภาครัฐที่มีภารกิจด้านการกำกับดูแลและส่งเสริมอุตสาหกรรมพื้นฐานและการเหมืองแร่ของประเทศ มีการจัดเก็บและใช้ประโยชน์ข้อมูลจำนวนมากในทุกมิติของภารกิจ ไม่ว่าจะเป็นข้อมูลใบอนุญาต ประทานบัตร อาชญาบัตร แหล่งแร่ สิ่งแวดล้อม และข้อมูลผู้ประกอบการ การบริหารจัดการข้อมูลเหล่านี้ให้มีคุณภาพ ปลอดภัย และพร้อมใช้งานจึงเป็นพื้นฐานสำคัญของการให้บริการประชาชนและการตัดสินใจเชิงนโยบาย

กพร. จึงได้จัดทำนโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูล (Data Governance Policy and Guidelines) ฉบับนี้ขึ้น โดยอ้างอิงกรอบกฎหมายและมาตรฐานที่เกี่ยวข้อง ดังนี้

๑. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ (พ.ร.บ. รัฐบาลดิจิทัล) มาตรา ๕ และมาตรา ๗ ซึ่งกำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายในการบริหารจัดการข้อมูล
๒. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ (มติ ครม. ๒๔ กุมภาพันธ์ พ.ศ. ๒๕๖๓)
๓. มาตรฐานรัฐบาลดิจิทัล ว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ จัดทำโดย สำนักงานพัฒนารัฐบาลดิจิทัล (สพร./DGA) ฉบับปรับปรุง พ.ศ. ๒๕๖๖
๔. มาตรฐานรัฐบาลดิจิทัล ว่าด้วยกรอบแนวทางการพัฒนามาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ (Thailand Government Information eXchange:TGIX)
๕. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (Personal Data Protection Act B.E. ๒๕๖๒ (๒๐๑๙))
๖. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
๗. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๘. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.๒๕๔๐ และ แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๒
๙. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔
๑๐. ประกาศ คณะกรรมการพัฒนารัฐบาลดิจิทัลเรื่องมาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ พ.ศ. ๒๕๖๓
๑๑. ประกาศ คณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่องมาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ พ.ศ. ๒๕๖๔
๑๒. พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙
๑๓. แนวนโยบายธนาคารแห่งประเทศไทยเรื่องการกำกับดูแลข้อมูล พ.ศ. ๒๕๖๔
๑๔. แผนยุทธศาสตร์ชาติ ๒๐ ปี พ.ศ. ๒๕๖๑ - ๒๕๘๐ และแผนปฏิรูปประเทศด้านการบริหารราชการแผ่นดิน ฉบับปรับปรุง
๑๕. เกณฑ์การประเมิน TRIS หัวข้อ P๑.๕ (Data Policy) และ P๒.๑ (Data Governance)

๑.๒ วัตถุประสงค์

นโยบายและแนวปฏิบัติฉบับนี้มีวัตถุประสงค์ ดังต่อไปนี้

๑. เพื่อกำหนดกรอบนโยบายข้อมูล (Data Policy) ครอบคลุมตลอดวงจรชีวิตข้อมูล ตั้งแต่การสร้าง จัดเก็บ ใช้งาน เผยแพร่ จัดเก็บในระยะยาว และทำลาย

๒. เพื่อกำหนดโครงสร้างการกำกับดูแลข้อมูล (Data Governance Structure) บทบาทหน้าที่ ความรับผิดชอบของผู้เกี่ยวข้องทุกระดับ

๓. เพื่อกำหนดแนวปฏิบัติที่เป็นรูปธรรม (Operational Guidelines) สำหรับการจัดทำบัญชีข้อมูล การควบคุมคุณภาพ ความมั่นคงปลอดภัย และการคุ้มครองข้อมูลส่วนบุคคล

๔. เพื่อเป็นเอกสารหลักฐานประกอบการตรวจประเมินองค์กรตามเกณฑ์ TRIS หัวข้อ P๑.๕ Data Policy

๕. เพื่อส่งเสริมให้ กพร. เป็นองค์กรที่ขับเคลื่อนด้วยข้อมูล (Data-Driven Organisation)

๑.๓ ขอบเขตการบังคับใช้

นโยบายและแนวปฏิบัติฉบับนี้มีผลบังคับใช้กับ

๑. ข้าราชการ ลูกจ้าง พนักงานราชการ และบุคคลที่ปฏิบัติงานให้แก่ กพร. ทุกคน

๒. หน่วยงานภายนอกที่ได้รับมอบหมาย จ้างเหมา หรือมีความสัมพันธ์ในการใช้ หรือ แลกเปลี่ยนข้อมูลกับ กพร.

๓. ระบบสารสนเทศ ฐานข้อมูล และข้อมูลทุกประเภทที่อยู่ในความครอบครองหรือความรับผิดชอบของ กพร. ทั้งในรูปแบบอิเล็กทรอนิกส์และเอกสาร

๔. ข้อมูลที่ กพร. รับมาจากหน่วยงานอื่น หรือส่งให้หน่วยงานอื่น

๑.๔ คำนิยาม

ในนโยบายและแนวปฏิบัติฉบับนี้ คำศัพท์ต่อไปนี้มีความหมายดังนี้

ตารางที่ ๑ นิยามศัพท์

คำศัพท์	คำนิยาม
API (Application Programming Interface)	ชุดคำสั่งและโปรโตคอลสำหรับการแลกเปลี่ยนข้อมูลระหว่างระบบสารสนเทศ ช่วยให้ระบบภายนอกเข้าถึงและใช้งานข้อมูลของหน่วยงานได้อย่างปลอดภัยและมีมาตรฐาน
Data Sharing Agreement (DSA)	ข้อตกลงการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ระบุเงื่อนไขการใช้งาน ขอบเขต ความรับผิดชอบ และมาตรการรักษาความปลอดภัยของคู่สัญญาทั้งสองฝ่าย
PDPA	พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ กำหนดหลักเกณฑ์การเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลอย่างมีธรรมาภิบาล
RoPA (Record of Processing Activities)	บันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล ประกอบด้วย วัตถุประสงค์ ประเภทข้อมูล ผู้รับข้อมูล ระยะเวลาเก็บรักษา และมาตรการรักษาความปลอดภัย
กพร.	กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่
การเข้าถึง	การเข้าสถานที่ การใช้งานทางอิเล็กทรอนิกส์ หรือกายภาพ รวมถึงการรับรู้ซึ่งข้อมูล
การควบคุมการเข้าถึง	การอนุญาต การกำหนดสิทธิและการเปลี่ยนแปลง การเพิกถอนหรือการยกเลิกสิทธิการเข้าถึง
ข้อมูล (Data)	สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
ข้อมูลหลัก (Master Data)	ข้อมูลอ้างอิงหลักขององค์กรที่ใช้ร่วมกันในระบบงานต่าง ๆ มีการเปลี่ยนแปลงน้อย และเป็นแหล่งข้อมูลเดียวที่ถูกต้องที่สุด (Single Source of Truth) เช่น ข้อมูลผู้ประกอบการ รหัสจังหวัด ประเภทแร่
คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)	คณะกรรมการธรรมาภิบาลข้อมูล ของ กพร.

คำศัพท์	คำนิยาม
คำอธิบายข้อมูล (Metadata)	ข้อมูลที่ใช้อธิบายข้อมูล ประกอบด้วยรายละเอียดเกี่ยวกับโครงสร้างของข้อมูล ความหมาย แหล่งที่มา รูปแบบการจัดเก็บ ผู้รับผิดชอบ วันที่จัดทำ การเชื่อมโยงของชุดข้อมูล และสิทธิในการเข้าถึงข้อมูล
คุณภาพข้อมูล (Data Quality)	ระดับความเหมาะสมของข้อมูลในการนำไปใช้งาน วัดตาม ๖ มิติ ได้แก่ ความถูกต้อง ความครบถ้วน ความสอดคล้อง ความเป็นปัจจุบัน ความตรงตามความต้องการ และความพร้อมใช้
เจ้าของข้อมูล (Data Owner)	บุคคลผู้ได้รับมอบอำนาจจากหัวหน้าหน่วยงานให้รับผิดชอบชุดข้อมูลของระบบงาน ซึ่งรวมถึงผู้บังคับบัญชาของเจ้าของข้อมูล มีหน้าที่กำหนดสิทธิการเข้าถึง มาตรฐานคุณภาพ และนโยบายการจัดการข้อมูลนั้น ๆ
ชั้นความลับข้อมูล (Data Classification)	การจำแนกระดับความสำคัญและข้อจำกัดในการเข้าถึงข้อมูล โดยแบ่งเป็นข้อมูลลับที่สุด ลับมาก ลับ และข้อมูลทั่วไป ตามระเบียบราชการ
ชุดข้อมูล (Dataset)	การนำข้อมูลจากหลายแหล่งมารวบรวมเพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล เช่น ชุดข้อมูลประทานบัตร ชุดข้อมูลผู้ประกอบการ
ธรรมาภิบาลข้อมูล (Data Governance)	การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอน เพื่อให้ข้อมูลมีคุณภาพ ปลอดภัย และสามารถเชื่อมโยงแลกเปลี่ยนได้
นโยบายข้อมูล (Data Policy)	เอกสารที่กำหนดหลักการ แนวทาง และกฎเกณฑ์ในการจัดการข้อมูลตลอดวงจรชีวิต ครอบคลุมการจัดชั้นความลับ การจัดเก็บ การประมวลผล การแลกเปลี่ยน และการเปิดเผยข้อมูล
บริกรข้อมูล (Data Steward)	บุคคลที่รับผิดชอบในการดูแลคุณภาพข้อมูล บัญชีข้อมูล และการปฏิบัติตามนโยบายในระดับปฏิบัติการ มีทั้งด้านธุรกิจ (Business Steward) ด้านเทคนิค (Technical Steward) และ ด้านคุณภาพข้อมูล (Quality Steward)
บัญชีข้อมูล (Data Catalog)	เอกสารแสดงบรรดารายการของชุดข้อมูลที่จำแนกแยกแยะ โดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงาน กพร.
บัญชีผู้ใช้ข้อมูล (User Account)	รายชื่อผู้มีสิทธิใช้ข้อมูล (User Name) และ รหัสผ่าน (Password) เพื่อการเข้าสู่ระบบคอมพิวเตอร์และระบบเครือข่ายหรือระบบสารสนเทศ
บันทึกเหตุการณ์ (Log)	ข้อมูลบันทึกเหตุการณ์ทางคอมพิวเตอร์หรือความปลอดภัยสารสนเทศ ได้แก่ บันทึกเหตุการณ์ของระบบ (System log) บันทึกการเข้าถึง (Access log) บันทึกการตรวจสอบ (Audit log) และ แฟ้มบันทึกเหตุการณ์ (Log file)

คำศัพท์	คำนิยาม
บุคคลภายนอก	ผู้ประกอบการหรือผู้ให้บริการภายนอก (Third Party) ผู้ร้องเรียนเรื่องราวต่าง ๆ ที่เกี่ยวข้องกับการทำงาน ของ กพร. โดยบุคคลภายนอกจะใช้ระบบสารสนเทศที่ กพร. เตรียมไว้ให้บริการสำหรับบุคคลภายนอก
บุคลากร	ผู้บริหาร ข้าราชการ พนักงานราชการและลูกจ้างของ กพร.
ผู้ควบคุมข้อมูล (Data Controller)	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
ผู้ใช้ข้อมูล (Data User)	บุคคลที่ได้รับอนุญาต (Authorised User) ให้สามารถเข้ามาใช้งาน บริหาร หรือ ดูแลรักษาระบบสารสนเทศของ กพร. ตามสิทธิและหน้าที่ความรับผิดชอบ
ผู้ดูแลระบบสารสนเทศ (System Administrator)	บุคลากรของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
ผู้ดูแลระบบ (Data Custodian)	ผู้รับผิดชอบด้านเทคนิคในการจัดเก็บ ดูแลรักษา และสำรองข้อมูลให้ระบบมีความพร้อมใช้งานและปลอดภัยตามมาตรฐานที่กำหนด
ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer: CIO)	ผู้บริหารระดับสูงที่รับผิดชอบด้านการกำกับดูแลเทคโนโลยีสารสนเทศของ กพร. ซึ่งครอบคลุม การกำกับดูแลข้อมูล และ การกำกับดูแลความปลอดภัย
ผู้สร้างข้อมูล (Data Creator)	บุคลากรของ กพร. ที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้ รวมทั้งมีหน้าที่ในการทำงานร่วมกับบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัยของข้อมูล
พจนานุกรมข้อมูล (Data Dictionary)	ตารางหรือข้อมูลที่ใช้อธิบายรายละเอียดของข้อมูลในแต่ละฟิลด์ ได้แก่ ชื่อฟิลด์ ประเภทข้อมูล ความยาว ความหมาย ค่าที่ยอมรับ และความสัมพันธ์กับข้อมูลอื่น
ระบบคอมพิวเตอร์	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่งชุดหรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
ระบบสารสนเทศ	ซอฟแวร์ระบบหรือซอฟแวร์ประยุกต์ที่ใช้ในการปฏิบัติงานของ กพร.

คำศัพท์	คำนิยาม
วงจรชีวิตข้อมูล (Data Lifecycle)	กระบวนการทั้งหมดของข้อมูลตั้งแต่การสร้าง (Create) จัดเก็บ (Store) ใช้งาน (Use) เผยแพร่ (Publish) จัดเก็บในระยะยาว (Archive) และทำลาย (Destroy)
ศสท.	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สารสนเทศ (Information)	ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งาน สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
สิทธิของผู้ใช้ข้อมูล	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของ กพร. โดย กพร. จะเป็นผู้พิจารณาสิทธิในการใช้งาน

กรอบธรรมาภิบาลข้อมูลของ กพร.

ภาพที่ ๑ กรอบธรรมาภิบาลข้อมูลของ กพร.

พันธกิจธรรมาภิบาลข้อมูล

๑. มีการจัดโครงสร้างองค์กรที่สอดรับกับธรรมาภิบาลข้อมูล
๒. สร้างข้อมูลที่มีคุณภาพและมีความน่าเชื่อถือในการใช้งานทั้งภายในและภายนอกองค์กร
๓. มีกระบวนการบริหารจัดการด้านข้อมูลในองค์กร
๔. มีการเสริมสร้างความรู้ความเข้าใจด้านการบริหารจัดการข้อมูลกับบุคลากรทุกระดับ
๕. ใช้เทคโนโลยีดิจิทัลมาสนับสนุนการทำงานด้านธรรมาภิบาลข้อมูลอย่างเหมาะสม

เป้าหมายธรรมาภิบาลข้อมูล

๑. มีคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) และผู้บริหารระดับสูง ด้านข้อมูล (Chief Information Officer: CIO)
๒. มีการกำหนดนโยบายด้านข้อมูลในแต่ละส่วนงานให้ครอบคลุมด้านคุณภาพข้อมูล การเชื่อมโยงข้อมูล และความมั่นคงปลอดภัยข้อมูล
๓. บุคลากรมีความรู้ความเข้าใจด้านการจัดการข้อมูลที่ดี เพื่อทำให้องค์กรไปสู่เป้าหมายร่วมกัน
๔. มีความร่วมมือด้านการแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก
๕. มีมาตรฐานการดำเนินการข้อมูลเปิด (Open Data)

ยุทธศาสตร์ธรรมาภิบาลข้อมูล

๑. กำหนดโครงสร้างธรรมาภิบาลข้อมูล
   ๑.๑. จัดตั้งคณะกรรมการธรรมาภิบาลข้อมูลและผู้บริหารระดับสูงด้านข้อมูล

๑.๒. มีการระบุหน้าที่ความรับผิดชอบของแต่ละส่วนงานด้านข้อมูล

๑.๓. มีการระบุหน้าที่ความรับผิดชอบของบริกรข้อมูล

๒. สร้างมาตรฐานธรรมาภิบาลข้อมูล

๒.๑. มีการกำหนดมาตรฐานในแต่ละส่วนงานให้ครอบคลุมด้านคุณภาพข้อมูล การเชื่อมโยงข้อมูล และความมั่นคงปลอดภัยข้อมูล

๒.๒. มีการกำหนดกระบวนการ ผู้รับผิดชอบ ข้อตกลงการให้บริการ และตัวชี้วัดในแต่ละส่วนงาน รวมถึงเกณฑ์การประเมินระดับบุคคลให้ครอบคลุมด้านคุณภาพข้อมูล การเชื่อมโยงข้อมูล และความมั่นคงปลอดภัยข้อมูล

๒.๓. มีการดำเนินการเพื่อรองรับมาตรฐานข้อมูลเปิดภาครัฐในอนาคต

๓. พัฒนาบุคลากรด้านธรรมาภิบาลข้อมูล

๓.๑. มีการสื่อสารองค์กรด้านจัดการข้อมูลที่ดี

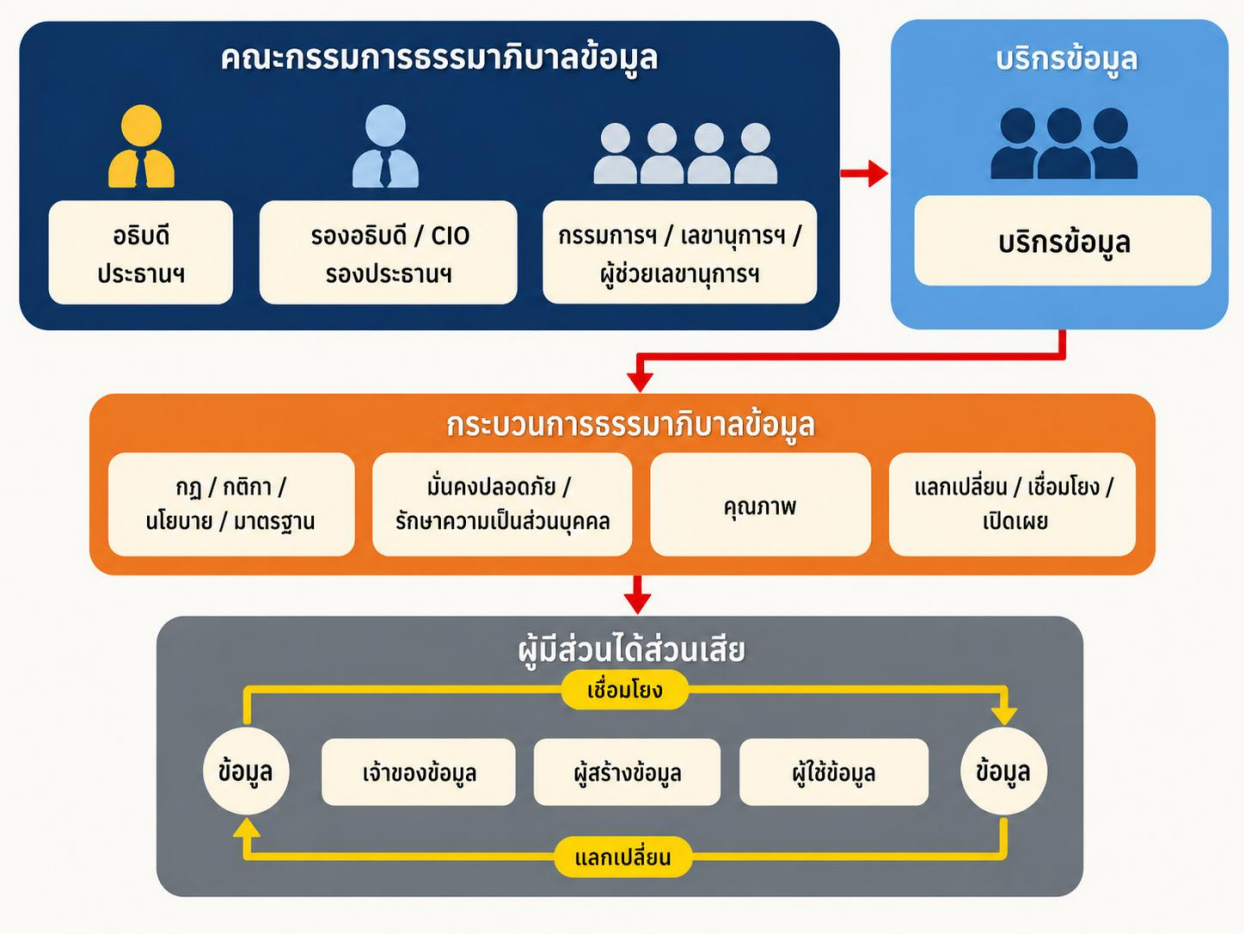
๓.๒. การฝึกอบรมเพื่อเสริมสร้างความรู้และทักษะของบุคลากร

บทที่ ๒ โครงสร้างการกำกับดูแลและบทบาทหน้าที่

การกำกับดูแลข้อมูลที่มีประสิทธิภาพต้องอาศัยโครงสร้างองค์กรที่ชัดเจน โดยกำหนดบทบาทหน้าที่และความรับผิดชอบของแต่ละระดับอย่างครบถ้วน บทนี้กำหนดโครงสร้างคณะกรรมการ บทบาทหน้าที่ และตาราง RACI Matrix สำหรับกิจกรรมหลักในวงจรชีวิตข้อมูล (ตอบเกณฑ์ TRIS P๒.๑.๑ และ P๒.๑.๓)

๒.๑ โครงสร้างการกำกับดูแลข้อมูล

กพร. กำหนดโครงสร้างการกำกับดูแลข้อมูลแบบลำดับชั้น (Hierarchical Governance) ดังนี้



ภาพที่ ๒ แผนผังโครงสร้างคณะกรรมการธรรมาภิบาลข้อมูล กพร.

ตารางที่ ๒ รายละเอียดของโครงสร้างการกำกับดูแลข้อมูล

ระดับ	คณะ/ตำแหน่ง	สังกัด
ระดับนโยบาย	คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee)	(๑) อธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ เป็น ประธานกรรมการ (๒) รองอธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ เป็น รองประธานกรรมการ (๓) ผู้อำนวยการกองทุกกอง ผู้อำนวยการกลุ่มตรวจสอบภายใน ผู้อำนวยการสำนักงานอุตสาหกรรมพื้นฐานและการเหมืองแร่ เขต ๑-๘ เป็น กรรมการ (๔) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสท.) เป็นกรรมการและเลขานุการ (๕) หัวหน้ากลุ่มสถิติและพัฒนาข้อมูล และหัวหน้ากลุ่มพัฒนาระบบเครือข่ายการสื่อสาร เป็นกรรมการและผู้ช่วยเลขานุการ
ระดับบริหาร	ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer - CIO)	รองอธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่
ระดับปฏิบัติการ	ทีมบริกรข้อมูล (Data Steward Team)	บุคลากรศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และผู้แทนแต่ละสำนักงานอุตสาหกรรมพื้นฐานและการเหมืองแร่เขต ๑-๘ ** แก้ไข
ระดับปฏิบัติการ	เจ้าของข้อมูล (Data Owner) ผู้สร้างข้อมูล (Data Creator) ผู้ใช้ข้อมูล (Data User)	(๑) ผู้อำนวยการกองทุกกอง (๒) ผู้อำนวยการสำนักงานอุตสาหกรรมพื้นฐานและการเหมืองแร่เขต ๑-๘ (๓) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (๔) เจ้าของระบบงาน
ระดับสนับสนุน	ผู้ดูแลระบบ (Data Custodian)	บุคลากรศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และเจ้าหน้าที่ผู้รับผิดชอบระบบ

๒.๒ บทบาทและความรับผิดชอบ

๒.๒.๑ คณะกรรมการธรรมาภิบาลข้อมูล

องค์ประกอบของคณะกรรมการธรรมาภิบาลข้อมูล

๑. ประธาน: อธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๒. รองประธาน: รองอธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)
๓. กรรมการ: ผู้อำนวยการกองทุกกอง ผู้อำนวยการกลุ่มตรวจสอบภายใน ผู้อำนวยการสำนักงานอุตสาหกรรมพื้นฐานและการเหมืองแร่เขต ๑-๘
๔. กรรมการและเลขานุการ: ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

อำนาจและหน้าที่ของคณะกรรมการ

๑. กำหนดและปรับปรุงนโยบาย แนวปฏิบัติ มาตรการ และกรอบการดำเนินงาน รวมถึงตรวจสอบและกำกับดูแลการดำเนินการด้านธรรมาภิบาลข้อมูลภาครัฐของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ให้สอดคล้องกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ
๒. กำหนดและปรับปรุงนโยบาย และแนวปฏิบัติ รวมถึงตรวจสอบและกำกับดูแลการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่
๓. กำหนดและปรับปรุงนโยบาย แนวปฏิบัติ และกรอบมาตรฐาน รวมถึงตรวจสอบและกำกับดูแลการดำเนินการ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ให้สอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
๔. แต่งตั้งคณะทำงาน เพื่อสนับสนุนการดำเนินงานด้านต่าง ๆ ตามที่คณะกรรมการมอบหมาย
๕. ปฏิบัติหน้าที่อื่นใดที่เกี่ยวข้องกับการดำเนินการด้านธรรมาภิบาลข้อมูลภาครัฐ การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๒.๒.๒ ผู้บริหารข้อมูลระดับสูง

CIO ทำหน้าที่รองประธานของคณะกรรมการธรรมาภิบาลข้อมูล มีหน้าที่

๑. ส่งเสริม ผลักดัน สนับสนุน ควบคุมการดำเนินงานตามธรรมาภิบาลข้อมูล
๒. กำหนดมาตรฐานข้อมูล แนวปฏิบัติ และเครื่องมือสนับสนุนการจัดการข้อมูล
๓. ประสานงานระหว่างคณะกรรมการและทีมบริกรข้อมูล
๔. รายงานสถานะการดำเนินงานต่อคณะกรรมการ
๕. จัดทำและทบทวนนโยบายข้อมูลอย่างน้อยปีละ ๑ ครั้ง

๒.๒.๓ เจ้าของข้อมูล และผู้ควบคุมข้อมูล

เจ้าของข้อมูล คือผู้อำนวยการสำนักงาน ผู้อำนวยการกอง ผู้อำนวยการศูนย์ที่รับผิดชอบระบบงานหรือชุดข้อมูลนั้น ๆ มีหน้าที่

๑. กำหนดสิทธิการเข้าถึงข้อมูล (Access Rights) ให้เหมาะสมกับหน้าที่
๒. กำหนดมาตรฐานคุณภาพและข้อกำหนดของข้อมูลในความรับผิดชอบ
๓. ตัดสินใจเกี่ยวกับการแบ่งปัน เปิดเผย หรือทำลายข้อมูล
๔. รับผิดชอบความถูกต้อง ครบถ้วน และเป็นปัจจุบันของข้อมูล
๕. กรณีเป็นข้อมูลส่วนบุคคล ทำหน้าที่ผู้ควบคุมข้อมูลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA)

๒.๒.๔ บริกรข้อมูล

บริกรข้อมูลแบ่งออกเป็น ๓ กลุ่ม

๑. บริกรข้อมูลด้านธุรกิจ (Business Data Steward): กำหนดและทบทวนความต้องการด้านคุณภาพข้อมูล จัดทำบัญชีข้อมูล กำหนดนิยาม Metadata รายงานผลลัพธ์ต่อคณะกรรมการ

๒. บริกรข้อมูลด้านเทคนิค (Technical Data Steward): ให้ข้อเสนอแนะเชิงเทคนิค ออกแบบระบบสารสนเทศให้รองรับคุณภาพและความปลอดภัย สนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศ

๓. บริกรข้อมูลด้านคุณภาพ (Data Quality Steward): วิเคราะห์และประเมินคุณภาพข้อมูล ตรวจสอบวัดผล และรายงานผลการดำเนินงาน

๒.๒.๕ ผู้ดูแลระบบ

ผู้ดูแลระบบมีหน้าที่รับผิดชอบด้านเทคนิค ดังนี้

๑. จัดเก็บ ดูแลรักษา และสำรองข้อมูลตามนโยบายที่กำหนด

๒. ควบคุมการเข้าถึงระบบสารสนเทศตามสิทธิที่ได้รับอนุมัติ

๓. รักษาความมั่นคงปลอดภัยของระบบและข้อมูล

๔. จัดทำและรักษาประวัติ (Log) การเข้าถึงระบบ

๒.๓ ตาราง RACI Matrix

ตาราง RACI Matrix แสดงความรับผิดชอบของแต่ละบทบาทในกิจกรรมหลักของวงจรชีวิตข้อมูล โดย อักษรแต่ละตัวมีความหมายดังนี้

R = Responsible ผู้รับผิดชอบดำเนินงาน

A = Accountable ผู้รับผิดชอบหลักและมีอำนาจตัดสินใจ

C = Consulted ผู้ให้คำปรึกษาหรือให้ความเห็น

I = Informed ผู้ที่ต้องได้รับแจ้งข้อมูล

ตารางที่ ๓ รายละเอียดตาราง RACI Matrix

กิจกรรม	คณะกรรมการ	CIO	Data Owner	Data Steward	Data Custodian
กำหนดนโยบายข้อมูล	A	R	C	C	I
จัดทำบัญชีข้อมูล (Data Catalog)	I	A	C	R	I
จำแนกชั้นความลับข้อมูล	A	C	R	R	I
ควบคุมคุณภาพข้อมูล	I	A	R	R	C
กำหนดสิทธิการเข้าถึง	I	C	A	C	R

กิจกรรม	คณะกรรมการ	CIO	Data Owner	Data Steward	Data Custodian
สำรองและกู้คืนข้อมูล	I	A	C	I	R
แลกเปลี่ยนข้อมูล (DSA/API)	A	C	R	C	I
คุ้มครองข้อมูลส่วนบุคคล (PDPA)	A	C	R	C	I
ตรวจสอบและวัดผล (Audit)	I	A	C	R	C
ทำลายข้อมูล (Destroy)	I	A	R	C	R

บทที่ ๓ นโยบายข้อมูลระดับองค์กร

นโยบายข้อมูลของ กพร. ครอบคลุมตลอดวงจรชีวิตข้อมูล ตั้งแต่การสร้าง จัดเก็บ ใช้งาน เผยแพร่ จัดเก็บระยะยาว ถึงการทำลาย โดยอ้างอิงกรอบธรรมาภิบาลข้อมูลภาครัฐของ DGA และตอบสนองต่อเกณฑ์ TRIS P๑.๕ (ตอบเกณฑ์ TRIS P๑.๕)

๓.๑ หมวดนโยบายทั่วไป และการจัดชั้นความลับข้อมูล

กพร. กำหนดนโยบายทั่วไปสำหรับการจัดการข้อมูลทุกประเภท ดังนี้

๓.๑.๑ หลักการทั่วไป

๑. ข้อมูลทุกชุดต้องได้รับการบริหารจัดการตามหลักธรรมาภิบาลข้อมูลภาครัฐ
๒. บุคลากรทุกคนมีหน้าที่รับผิดชอบในการดูแลรักษาความถูกต้อง ครบถ้วน และปลอดภัยของข้อมูลที่ตนรับผิดชอบ
๓. การเข้าถึงข้อมูลต้องเป็นไปตามสิทธิที่ได้รับอนุมัติ โดยยึดหลัก Need-to-Know (หลักการให้เข้าถึงข้อมูลเฉพาะเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น แม้บุคคลนั้นจะอยู่ในหน่วยงานเดียวกัน ก็ไม่ควรเห็นข้อมูลที่ไม่เกี่ยวข้องกับหน้าที่ของตน) และ Least Privilege (หลักการกำหนดสิทธิการใช้งานให้น้อยที่สุดเท่าที่จำเป็นต่อการทำงาน เช่น ให้สิทธิอ่าน แก้ไข อนุมัติ หรือดูแลระบบ เฉพาะในระดับที่จำเป็น และต้องทบทวนหรือยกเลิกสิทธิเมื่อหมดความจำเป็น)
๔. ต้องมีการบันทึก Log การเข้าถึงและแก้ไขข้อมูลสำคัญทุกครั้ง
๕. นโยบายต้องได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ

๓.๑.๒ การจัดชั้นความลับข้อมูล

กพร. กำหนดการจัดชั้นความลับข้อมูลตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ แบ่งเป็น ๔ ระดับ ดังนี้

ตารางที่ ๔ รายละเอียดชั้นความลับข้อมูล

ชั้นความลับ	ความหมาย	ตัวอย่างข้อมูลของ กพร.	มาตรการควบคุม
ลับที่สุด	หากเปิดเผยจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุดต่อความมั่นคงชาติ	ข้อมูลพิกัดแหล่งแร่เชิงยุทธศาสตร์	เข้ารหัสสูงสุด เข้าถึงได้เฉพาะผู้บริหารระดับสูงและผู้ได้รับมอบอำนาจพิเศษ
ลับมาก	หากเปิดเผยจะก่อให้เกิดความเสียหายอย่างร้ายแรง	ข้อมูลการตรวจสอบสถานประกอบการ	เข้ารหัส เข้าถึงเฉพาะระดับบริหารและเจ้าของงาน
ลับ	หากเปิดเผยจะก่อให้เกิดความเสียหาย	ข้อมูลการร้องเรียน ข้อมูลบุคลากร	ควบคุมสิทธิ Log การเข้าถึง
ทั่วไป	ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ได้	สถิติแร่ รายชื่อผู้ประกอบการที่เปิดเผย	ไม่มีข้อจำกัดพิเศษ อาจเผยแพร่เป็น Open Data

๓.๒ หมวดนโยบายการจัดเก็บและทำลายข้อมูล

กพร. กำหนดนโยบายการจัดเก็บและทำลายข้อมูล เพื่อให้ข้อมูลมีความพร้อมใช้งาน ปลอดภัย และบริหารจัดการพื้นที่จัดเก็บอย่างมีประสิทธิภาพ

๓.๒.๑ การจัดเก็บข้อมูล

๑. ข้อมูลสำคัญต้องจัดเก็บในระบบที่ได้รับการรับรองความมั่นคงปลอดภัยตามมาตรฐาน
๒. ต้องมีการสำรองข้อมูล (Backup) สำหรับระบบสำคัญ ความถี่ขึ้นอยู่กับระดับความสำคัญ ได้แก่ ระบบสำคัญสูงสำรองทุกวัน ระบบทั่วไปสำรองทุกสัปดาห์
๓. ระบบสำรองต้องอยู่ในพื้นที่แยกจากระบบหลัก (Offsite Backup) และทดสอบการกู้คืนอย่างน้อยเดือนละ ๑ ครั้ง
๔. การจัดเก็บข้อมูลต้องมีระยะเวลาที่จำกัด และเก็บเท่าที่จำเป็นต่อการดำเนินงานตามภารกิจของ กพร. เท่านั้น
๕. ระยะเวลาการจัดเก็บข้อมูลต้องมีความสอดคล้องกับกฎหมายและระเบียบที่เกี่ยวข้อง เช่น ข้อมูลทางการเงินเก็บไม่น้อยกว่า ๕ ปี
๖. ข้อมูลที่หยุดใช้งานเกิน ๕ ปีให้ประเมินว่ายังมีความจำเป็นในการจัดเก็บหรือไม่ ถ้าไม่จำเป็นควรทำลายทิ้ง แต่ถ้าจำเป็นให้ย้ายไปเก็บในสื่อจัดเก็บระยะยาว (Archive) พร้อมบันทึกรายการ

๓.๒.๒ การทำลายข้อมูล

๑. การทำลายข้อมูลต้องได้รับความเห็นชอบจากเจ้าของข้อมูลและผู้บริหารที่มีอำนาจอนุมัติ
๒. วิธีการทำลายข้อมูลต้องเหมาะสมกับสื่อบันทึก ได้แก่ กระดาษใช้เครื่องหั่นทำลาย ฮาร์ดดิสก์ใช้การ Format ตามมาตรฐาน DOD ๕๒๒๐.๒๒-M แผ่น CD/DVD ใช้เครื่องหั่น

๓. ต้องจัดทำบันทึกการทำลายข้อมูล ระบุ วัน/เวลา ประเภทข้อมูล ปริมาณ วิธีการ และผู้รับผิดชอบ

๓.๓ หมวดนโยบายการประมวลผลและการใช้ข้อมูล

๑. การใช้ข้อมูลต้องเป็นไปเพื่อปฏิบัติภารกิจของ กพร. เท่านั้น ห้ามใช้เพื่อประโยชน์ส่วนตัวหรือนอกขอบเขตที่ได้รับอนุญาต
๒. การประมวลผลข้อมูลส่วนบุคคลต้องมีฐานกฎหมายรองรับตาม PDPA และจัดทำ RoPA ครบถ้วน
๓. ห้ามนำข้อมูลลับออกจากระบบโดยไม่ได้รับอนุญาต ไม่ว่าจะเป็นการคัดลอก พิมพ์ หรือส่งทางอิเล็กทรอนิกส์
๔. การนำข้อมูลไปใช้ร่วมกับ AI หรือระบบวิเคราะห์ข้อมูลขั้นสูงต้องผ่านการประเมินความเสี่ยงด้านความเป็นส่วนตัวก่อน
๕. ต้องมีการบันทึก Log การใช้งานข้อมูลสำคัญเพื่อให้สามารถตรวจสอบย้อนหลังได้

๓.๔ หมวดนโยบายการแลกเปลี่ยนและเชื่อมโยงข้อมูล

๑. การแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอกต้องจัดทำ Data Sharing Agreement (DSA) ก่อนทุกครั้ง
๒. DSA ต้องระบุวัตถุประสงค์ ขอบเขต ประเภทข้อมูล ระยะเวลา มาตรการรักษาความปลอดภัย และความรับผิดชอบของคู่สัญญา
๓. การเชื่อมโยงข้อมูลผ่าน API ต้องใช้มาตรฐาน REST API หรือ Web Service ที่ได้รับการรับรองความปลอดภัย พร้อม Authentication ที่แข็งแกร่ง
๔. ต้องมีการทดสอบและตรวจสอบความถูกต้องของข้อมูลก่อนและหลังการแลกเปลี่ยน
๕. บันทึก Log การแลกเปลี่ยนข้อมูลทุกครั้ง และรายงานให้ CIO ทราบ

๓.๕ หมวดนโยบายการเปิดเผยข้อมูล

๑. ข้อมูลทั่วไป (ไม่มีชั้นความลับ) ที่ไม่กระทบต่อความเป็นส่วนตัวของบุคคล สามารถเปิดเผยเป็น Open Data ผ่านช่องทางที่กำหนด เช่น เว็บไซต์ data.go.th
๒. ก่อนเปิดเผยข้อมูล ต้องผ่านกระบวนการตรวจสอบ: ชั้นความลับ ข้อมูลส่วนบุคคล และสิทธิทางกฎหมาย
๓. ข้อมูลที่ถูกร้องขอตาม พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ ต้องดำเนินการตามขั้นตอนที่กฎหมายกำหนด
๔. ต้องจัดทำบัญชีรายการชุดข้อมูล Open Data ของ กพร. และเผยแพร่ผ่าน ศูนย์กลางข้อมูลเปิดภาครัฐ (Open Government Data) บนเว็บไซต์ data.go.th อย่างน้อยตามที่ DGA กำหนด
๕. การเปิดเผยข้อมูลส่วนบุคคลให้ผู้ประมวลผลข้อมูลส่วนบุคคล ต้องจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลกับผู้ประมวลผลข้อมูลส่วนบุคคลเพื่อให้สอดคล้องกับ PDPA

บทที่ ๔ แนวปฏิบัติธรรมาภิบาลข้อมูลตลอดวงจรชีวิต

บทนี้กำหนดแนวปฏิบัติที่เป็นรูปธรรม (How-to Guidelines) สำหรับกิจกรรมหลัก ๕ ด้าน ครอบคลุมตลอดวงจรชีวิตข้อมูล ตอบเกณฑ์ TRIS P๒.๑.๓ อย่างครบถ้วน

๔.๑ แนวปฏิบัติการจัดทำบัญชีข้อมูล

การจัดทำบัญชีข้อมูลเป็นกิจกรรมพื้นฐานสำคัญที่ทำให้ กพร. รู้ว่ามีข้อมูลอะไรอยู่ที่ไหน ใครเป็นเจ้าของ และพร้อมใช้งานมากน้อยเพียงใด

๔.๑.๑ ขั้นตอนการจัดทำบัญชีข้อมูล

๑. สำรวจกระบวนการและชุดข้อมูล: ระบุชุดข้อมูลทั้งหมดของ กพร. จากทุกระบบงาน พร้อมแหล่งที่มา รูปแบบการจัดเก็บ และความถี่ในการปรับปรุง
๒. จำแนกและจัดกลุ่มข้อมูล: แบ่งชุดข้อมูลตามหมวดหมู่ภารกิจ (การอนุญาต สิ่งแวดล้อม บริหาร ฯลฯ) และกำหนดชั้นความลับ
๓. จัดทำ Metadata: บันทึกคำอธิบายข้อมูลตามมาตรฐาน ๑๔ ฟิลด์บังคับของ DGA (ดูตารางที่ ๕ ด้านล่าง)
๔. จัดทำ Data Dictionary: อธิบายรายละเอียดของแต่ละฟิลด์ข้อมูล
๕. เผยแพร่และบำรุงรักษา: เผยแพร่บัญชีข้อมูลผ่านระบบ Data Catalog และปรับปรุงเมื่อมีการเปลี่ยนแปลง

๔.๑.๒ โครงสร้างมาตรฐาน Metadata ๑๔ ฟิลด์บังคับตามมาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัล (DGA)

ตารางที่ ๕ โครงสร้างมาตรฐาน Metadata ๑๔ ฟิลด์บังคับตามมาตรฐานของ DGA

ลำดับ	ฟิลด์ Metadata	คำอธิบาย	ตัวอย่าง
๑	ชื่อชุดข้อมูล	ชื่อที่สื่อความหมายของชุดข้อมูล	ข้อมูลประทานบัตรเหมืองแร่
๒	หน่วยงาน	หน่วยงานเจ้าของชุดข้อมูล	กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่
๓	คำอธิบาย	รายละเอียดเนื้อหาของชุดข้อมูล	ข้อมูลการออกประทานบัตรเหมืองแร่ทั่วประเทศ
๔	หมวดหมู่	หมวดหมู่หลักของชุดข้อมูล	อุตสาหกรรมและการเหมืองแร่
๕	คำสำคัญ	คำค้นหาที่เกี่ยวข้อง	ประทานบัตร แร่ เหมือง
๖	วันที่สร้าง	วันที่เริ่มจัดทำชุดข้อมูล	๐๑/๐๑/๒๕๖๐
๗	วันที่ปรับปรุง	วันที่แก้ไขข้อมูลล่าสุด	๐๑/๐๔/๒๕๖๘
๘	ความถี่การปรับปรุง	ความถี่ในการอัปเดตข้อมูล	รายวัน/รายเดือน/รายปี

ลำดับ	ฟิลด์ Metadata	คำอธิบาย	ตัวอย่าง
๙	รูปแบบไฟล์	รูปแบบที่จัดเก็บ	CSV, JSON, XML
๑๐	ผู้รับผิดชอบ	ชื่อผู้ดูแลชุดข้อมูล	กลุ่มสารสนเทศเหมืองแร่
๑๑	สิทธิการเข้าถึง	ระดับการเปิดเผย	สาธารณะ/ภายใน/ลับ/ลับมาก/ลับที่สุด
๑๒	ขอบเขต	ขอบเขตทางภูมิศาสตร์หรือเวลา	ทั่วประเทศ ปี ๒๕๔๐-ปัจจุบัน
๑๓	มาตรฐานที่ใช้	มาตรฐานหรือกฎหมายที่เกี่ยวข้อง	พ.ร.บ. แร่ พ.ศ. ๒๕๖๐
๑๔	การเชื่อมโยง	ความสัมพันธ์กับชุดข้อมูลอื่น	เชื่อมกับข้อมูลอาชญาบัตร

๔.๒ แนวปฏิบัติการควบคุมคุณภาพข้อมูล

การควบคุมคุณภาพข้อมูลวัดตาม ๖ มิติหลัก พร้อมวิธีการตรวจสอบที่เป็นรูปธรรม

๔.๒.๑ มิติคุณภาพข้อมูล ๖ ด้าน

ตารางที่ ๖ มิติคุณภาพข้อมูล ๖ ด้าน

มิติ	คำอธิบาย	วิธีตรวจสอบ	KPI เป้าหมาย
ความถูกต้อง (Accuracy)	ข้อมูลตรงกับความเป็นจริง ไม่มีความผิดพลาด	Cross-check กับแหล่งข้อมูลต้นทาง สุ่มตรวจรายการ	>= ๙๘%
ความครบถ้วน (Completeness)	ข้อมูลมีครบทุกฟิลด์ที่จำเป็นไม่มีค่าว่างที่ไม่ควรว่าง	นับ NULL/Blank ในฟิลด์สำคัญ	>= ๙๕%
ความสอดคล้อง (Consistency)	ข้อมูลชุดเดียวกันตรงกันในทุกระบบ ไม่ขัดแย้งกัน	เปรียบเทียบข้อมูลระหว่างระบบ	>= ๙๕%
ความเป็นปัจจุบัน (Timeliness)	ข้อมูลอัปเดตทันเวลาตามที่กำหนด	ตรวจสอบวันที่ปรับปรุงล่าสุด	ตามความถี่ที่กำหนด
ความตรงตามความต้องการ (Relevancy)	ข้อมูลตอบสนองความต้องการของผู้ใช้งาน	สำรวจความพึงพอใจผู้ใช้ประจำปี	>= ๘๐% พึงพอใจ
ความพร้อมใช้ (Availability)	ระบบข้อมูลพร้อมให้บริการตามเวลาที่กำหนด	วัด System Uptime	>= ๙๙.๕% Uptime

๔.๒.๒ กระบวนการควบคุมคุณภาพข้อมูล

๑. กำหนดมาตรฐานคุณภาพ: เจ้าของข้อมูลกำหนดเกณฑ์ขั้นต่ำของคุณภาพข้อมูลในแต่ละด้าน เช่น ความถูกต้อง ความครบถ้วน ความเป็นปัจจุบัน และความสอดคล้องของข้อมูล เพื่อให้ทุกหน่วยงานใช้เป็นมาตรฐานเดียวกัน
๒. ตรวจสอบเมื่อมีข้อมูลใหม่: เมื่อมีการนำเข้าข้อมูลใหม่ ให้ตรวจสอบทันทีตามเงื่อนไขหรือกฎที่กำหนดไว้ เช่น รูปแบบข้อมูลต้องถูกต้อง ข้อมูลสำคัญต้องไม่ว่าง และค่าข้อมูลต้องอยู่ในช่วงที่ยอมรับได้
๓. ตรวจสอบสม่ำเสมอ: บริกรข้อมูลหรือผู้รับผิดชอบคุณภาพข้อมูลสุ่มตรวจสอบข้อมูลเป็นรายเดือน เพื่อค้นหาความผิดพลาดที่อาจไม่พบในขั้นตอนนำเข้าข้อมูล และป้องกันปัญหาสะสมในระยะยาว
๔. รายงานปัญหา: เมื่อพบปัญหาคุณภาพข้อมูล ให้บันทึกรายละเอียดในระบบติดตามปัญหา พร้อมแจ้งเจ้าของข้อมูลให้รับทราบ เพื่อให้สามารถตรวจสอบสาเหตุและวางแผนแก้ไขได้อย่างเป็นระบบ
๕. แก้ไขและยืนยันผล: เจ้าของข้อมูลดำเนินการแก้ไขปัญหา และยืนยันความถูกต้องของข้อมูล ภายในระยะเวลาที่กำหนดตามข้อตกลงการให้บริการ เพื่อให้ข้อมูลกลับมาใช้งานได้อย่างน่าเชื่อถือ
๖. รายงานผลต่อ CIO: จัดทำรายงานสรุปคุณภาพข้อมูลเป็นรายไตรมาสเสนอต่อ CIO และคณะกรรมการธรรมาภิบาลข้อมูล เพื่อใช้ติดตามสถานะ ปัญหาสำคัญ แนวโน้มคุณภาพข้อมูล และแนวทางปรับปรุงในภาพรวม

๔.๓ แนวปฏิบัติการรักษาความมั่นคงปลอดภัย

กพร. กำหนดมาตรการรักษาความมั่นคงปลอดภัยข้อมูลแบบหลายชั้น (Defense in Depth) โดยอ้างอิงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐

๔.๓.๑ การควบคุมสิทธิการเข้าถึง

๑. ใช้หลักการ Least Privilege: ผู้ใช้ได้รับสิทธิเท่าที่จำเป็นสำหรับปฏิบัติงานเท่านั้น
๒. กำหนดสิทธิตามบทบาท (Role-Based Access Control) ทบทวนสิทธิอย่างน้อยปีละ ๑ ครั้ง
๓. ยกเลิกสิทธิทันทีเมื่อพนักงานลาออก เปลี่ยนตำแหน่ง หรือสิ้นสุดการจ้าง ภายใน ๓ วัน
๔. บังคับใช้ Password Policy: ความยาวขั้นต่ำ ๘ ตัวอักษร ประกอบด้วยตัวพิมพ์ใหญ่ ตัวเลข สัญลักษณ์ และเปลี่ยนทุก ๓-๖ เดือน
๕. ระบบสำคัญต้องใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication)

๔.๓.๒ การเข้ารหัส

๑. ข้อมูลลับและข้อมูลส่วนบุคคลต้องเข้ารหัสทั้งในสถานะจัดเก็บ (At Rest) และระหว่างส่ง (In Transit)
๒. ใช้มาตรฐานการเข้ารหัสขั้นต่ำ AES-๒๕๖ สำหรับ At Rest และ TLS ๑.๒ ขึ้นไปสำหรับ In Transit
๓. การส่งข้อมูลนอกเครือข่ายต้องผ่าน VPN หรือช่องทางที่เข้ารหัสเสมอ

๔.๓.๓ การจัดเก็บ Log Files

๑. จัดเก็บ Log การเข้าถึงระบบ การแก้ไขข้อมูล และเหตุการณ์ด้านความปลอดภัยไม่น้อยกว่า ๙๐ วัน
๒. ห้ามผู้ดูแลระบบแก้ไข Log ยกเว้นผู้ตรวจสอบที่ได้รับมอบหมาย
๓. ทบทวน Log เป็นประจำเพื่อตรวจหาพฤติกรรมผิดปกติ

๔.๔ แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

กพร. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ต้องปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ อย่างเคร่งครัด

๔.๔.๑ การจัดทำ Privacy Notice

๑. ประกาศนโยบายความเป็นส่วนตัว (Privacy Notice) ชัดเจน ก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล
๒. ระบุ วัตถุประสงค์ ฐานกฎหมาย ประเภทข้อมูล ระยะเวลาเก็บ สิทธิของเจ้าของข้อมูล และช่องทางติดต่อ
๓. เผยแพร่ผ่านเว็บไซต์ กพร. และจุดรับบริการที่เกี่ยวข้อง

๔.๔.๒ การขอความยินยอม

๑. ขอความยินยอมก่อนเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ยกเว้นกรณีมีฐานกฎหมายอื่นรองรับ
๒. บันทึกความยินยอม วัน/เวลา วิธีการ และขอบเขต
๓. เจ้าของข้อมูลสามารถถอนความยินยอมได้ตลอดเวลา

๔.๔.๓ การจัดทำ RoPA

๑. จัดทำบันทึกกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA) ครบทุกระบบงานที่มีการประมวลผลข้อมูลส่วนบุคคล
๒. RoPA ต้องประกอบด้วย วัตถุประสงค์ ประเภทข้อมูล ผู้รับข้อมูล ระยะเวลาเก็บ มาตรการความปลอดภัย
๓. ทบทวนและปรับปรุง RoPA อย่างน้อยปีละ ๑ ครั้ง

๔.๔.๔ แผนรับมือข้อมูลรั่วไหล

๑. ตรวจพบเหตุ: ผู้ดูแลระบบหรือผู้ใช้แจ้งเหตุต้องสงสัยทันที
๒. ประเมินเบื้องต้น: ผู้ดูแลระบบประเมินขอบเขตและความรุนแรงภายใน ๒๔ ชั่วโมง
๓. แจ้งผู้บริหาร: รายงาน CIO และคณะกรรมการธรรมาภิบาลข้อมูลทันที
๔. แจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.): หากเข้าข่ายต้องแจ้ง สคส. จะต้องดำเนินการภายใน ๗๒ ชั่วโมงตามกฎหมาย
๕. แจ้งเจ้าของข้อมูล: แจ้งเจ้าของข้อมูลที่ได้รับผลกระทบโดยไม่ชักช้า
๖. จัดทำรายงานและป้องกัน: สรุปเหตุการณ์ มาตรการแก้ไข และแผนป้องกันซ้ำ

๔.๕ แนวปฏิบัติการเปิดเผยและแลกเปลี่ยนข้อมูล

กพร. กำหนดกระบวนการการทำ Data Sharing Agreement (DSA) และการเชื่อมโยงผ่าน API อย่างเป็นระบบ

๔.๕.๑ กระบวนการจัดทำ Data Sharing Agreement (DSA)

๑. ยื่นคำขอ: หน่วยงานที่ต้องการข้อมูลยื่นคำขอแลกเปลี่ยนข้อมูลอย่างเป็นทางการ พร้อมระบุวัตถุประสงค์และประเภทข้อมูลที่ต้องการ

๒. ประเมินความเหมาะสม: เจ้าของข้อมูลและ CIO พิจารณาความเหมาะสม ชั้นความลับ และความเป็นส่วนตัว (PDPA)
๓. ร่าง DSA: ระบุเงื่อนไขการใช้งาน ขอบเขต ระยะเวลา มาตรการรักษาความปลอดภัย และข้อห้าม
๔. อนุมัติ: CIO และผู้บริหารที่มีอำนาจอนุมัติ DSA
๕. ดำเนินการ: จัดเตรียมช่องทางการเข้าถึง (API/SFTP/ฯลฯ) และฝึกอบรมผู้ใช้
๖. ติดตามและทบทวน: ตรวจสอบการใช้งานตาม Log ทบทวน DSA อย่างน้อยปีละ ๑ ครั้ง

๔.๕.๒ มาตรฐานการเชื่อมโยงผ่าน API

๑. ใช้มาตรฐาน REST API ตาม DGA API Standard
๒. กำหนดให้มีการยืนยันตัวตนก่อนเข้าใช้งานระบบหรือเชื่อมต่อ API ทุกครั้ง โดยใช้มาตรฐาน OAuth ๒.๐ หรือ API Key ที่มีการจัดการอย่างปลอดภัย เช่น การกำหนดสิทธิการเข้าถึง การเข้ารหัส การจำกัดอายุการใช้งาน และการเพิกถอนเมื่อไม่จำเป็นหรือพบความเสี่ยง
๓. กำหนดขีดจำกัดจำนวนครั้งหรือปริมาณการเรียกใช้งานระบบหรือ API ภายในช่วงเวลาที่เหมาะสม เพื่อป้องกันการใช้งานเกินกว่าที่กำหนด ลดความเสี่ยงจากการโจมตีแบบถี่ ๆ และรักษาเสถียรภาพของระบบ
๔. จัดทำเอกสาร API Documentation ให้ครบถ้วนและเป็นปัจจุบัน เพื่อให้หน่วยงานที่ต้องการเชื่อมต่อสามารถใช้งานได้อย่างถูกต้อง ปลอดภัย และสอดคล้องกับข้อกำหนดของระบบ โดยควรระบุรายละเอียดสำคัญ เช่น วัตถุประสงค์การใช้งาน รูปแบบการเรียกใช้ API โครงสร้างข้อมูล วิธีการยืนยันตัวตน สิทธิการเข้าถึง ตัวอย่าง Request และ Response รหัสข้อผิดพลาด และช่องทางติดต่อผู้ดูแลระบบ
๕. ทดสอบความปลอดภัย API Security อย่างน้อยปีละ ๑ ครั้ง

บทที่ ๕ การตรวจสอบ วัดผล และการปรับปรุงอย่างต่อเนื่อง

การตรวจสอบและวัดผลอย่างสม่ำเสมอเป็นกลไกสำคัญที่ทำให้ธรรมาภิบาลข้อมูลของ กพร. มีประสิทธิผลและพัฒนาอย่างต่อเนื่อง บทนี้กำหนดกรอบการประเมิน KPI และกระบวนการปรับปรุง (ตอบเกณฑ์ TRIS P๒.๑.๔)

๕.๑ การประเมินความพร้อมของหน่วยงาน

กพร. ใช้เกณฑ์ระดับความพร้อมธรรมาภิบาลข้อมูล ๐-๕ ระดับ เพื่อประเมินสถานะปัจจุบันและกำหนดเป้าหมายการพัฒนา

ตารางที่ ๗ รายละเอียดเกณฑ์การประเมินความพร้อม

ระดับ	ชื่อระดับ	ลักษณะ	เป้าหมาย กพร.
๐	Initial (เริ่มต้น)	ไม่มีนโยบายหรือกระบวนการชัดเจน จัดการข้อมูลตามดุลยพินิจบุคคล	-
๑	Managed (จัดการได้)	มีนโยบายบางส่วน มีกระบวนการเบื้องต้น แต่ยังไม่ครบถ้วน	ผ่านพ้น
๒	Defined (กำหนดชัด)	มีนโยบายและกระบวนการเป็นลายลักษณ์อักษร ปฏิบัติสม่ำเสมอ	ปัจจุบัน
๓	Measured (วัดผลได้)	มีการวัดผลและรายงานตามตัวชี้วัด ปรับปรุงตามข้อมูล	เป้าหมาย ๑ ปี
๔	Optimised (เพิ่มประสิทธิภาพ)	ปรับปรุงอย่างต่อเนื่อง ใช้ข้อมูลเชิงลึกในการพัฒนา	เป้าหมาย ๓ ปี
๕	Innovating (นวัตกรรม)	ผู้นำในการใช้ข้อมูลเพื่อสร้างนวัตกรรมบริการสาธารณะ	เป้าหมายระยะยาว

กพร. กำหนดให้ประเมิน Readiness Assessment ปีละ ๑ ครั้ง โดย CIO รายงานผลต่อคณะกรรมการพร้อมแผนพัฒนาไปสู่ระดับถัดไป

๕.๒ ดัชนีชี้วัด (KPIs) ด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย

ตารางที่ ๘ KPIs ด้านคุณภาพข้อมูล

ตัวชี้วัด (KPI)	สูตรคำนวณ	เป้าหมาย	ความถี่วัด
ความถูกต้องข้อมูล	(รายการถูกต้อง / รายการทั้งหมด) × ๑๐๐	>= ๙๘%	รายเดือน
ความครบถ้วน Metadata	(ชุดข้อมูลที่มี Metadata ครบ / ทั้งหมด) × ๑๐๐	>= ๙๐%	รายไตรมาส
การปรับปรุงข้อมูลทันเวลา	(ชุดข้อมูลที่อัปเดตตามกำหนด / ทั้งหมด) × ๑๐๐	>= ๙๕%	รายเดือน
อัตราการแก้ไขปัญหาคุณภาพ	(ปัญหาที่แก้ไขใน SLA / ทั้งหมด) × ๑๐๐	>= ๙๐%	รายเดือน

ตารางที่ ๙ KPIs ด้านความมั่นคงปลอดภัย

ตัวชี้วัด (KPI)	เป้าหมาย	ความถี่วัด
System Uptime ของระบบสำคัญ	>= ๙๙.๕%	รายเดือน
ระยะเวลากู้คืนระบบ (RTO)	<= ๔ ชั่วโมงสำหรับระบบสำคัญ	ทดสอบรายปี
การทบทวนสิทธิการเข้าถึง	๑๐๐% ของบัญชีผู้ใช้ภายใน ๓๐ วันจากวันครบรอบ	รายปี
เหตุการณ์ละเมิดความปลอดภัย	๐ เหตุการณ์ร้ายแรง ≤ ๕ เหตุการณ์เล็กน้อย/ปี	รายปี
การสำรองข้อมูลสำเร็จ	>= ๙๙% ของการสำรองข้อมูลตามกำหนด	รายสัปดาห์
การฝึกอบรม PDPA/Security	๑๐๐% ของบุคลากรอบรมครบภายใน ๑ ปี	รายปี

ตารางที่ ๑๐ ความถี่ในการตรวจสอบ

ประเภทการตรวจสอบ	ความถี่	ผู้รับผิดชอบ	ผู้รับรายงาน
ตรวจสอบคุณภาพข้อมูล (Data Quality Audit)	รายเดือน	Data Quality Steward	CIO
ทบทวนสิทธิการเข้าถึง (Access Review)	ปีละ ๑ ครั้ง	ผู้ดูแลระบบ + เจ้าของข้อมูล	CIO

ประเภทการตรวจสอบ	ความถี่	ผู้รับผิดชอบ	ผู้รับรายงาน
ตรวจสอบความมั่นคงปลอดภัย (Security Audit)	ปีละ ๑ ครั้ง	ผู้ตรวจสอบภายใน/ภายนอก	คณะกรรมการ
ประเมินความเสี่ยง (Risk Assessment)	ปีละ ๑ ครั้ง	ทีม IT + ผู้ตรวจสอบ	คณะกรรมการ
ทดสอบการกู้คืนข้อมูล (DR Test)	ปีละ ๑ ครั้ง	ผู้ดูแลระบบ	CIO
ตรวจสอบ PDPA Compliance	ปีละ ๑ ครั้ง	DPO/ผู้ตรวจสอบ	คณะกรรมการ
ทบทวนบัญชีข้อมูล (Catalog Review)	รายไตรมาส	Business Data Steward	CIO

๕.๓ กระบวนการปรับปรุงและรายงานผู้บริหาร

๕.๓.๑ รอบการประชุมทบทวน (Review Cycle)

ตารางที่ ๑๑ รอบการประชุมทบทวน

ระดับ	ความถี่	หัวข้อหลัก	ผลลัพธ์ที่คาดหวัง
ระดับปฏิบัติการ (CIO + Stewards)	รายเดือน	สถานะ KPI คุณภาพข้อมูล ปัญหาที่พบ	แผนแก้ไขระยะสั้น
ระดับบริหาร (CIO รายงานต่อผู้บริหาร)	รายไตรมาส	ผล KPI สรุป ความเสี่ยง ความคืบหน้าโครงการ	การตัดสินใจ ทรัพยากร
ระดับนโยบาย (คณะกรรมการ)	ปีละ ๒ ครั้ง (มิ.ย. และ ธ.ค.)	ผลประเมินประจำปี แผนพัฒนา การทบทวนนโยบาย	อนุมัตินโยบาย แผนปีถัดไป

๕.๓.๒ หัวข้อที่ต้องมีในรายงานประจำปีต่อคณะกรรมการ

๑. สรุปผล KPI ทุกตัวชี้วัด เปรียบเทียบกับเป้าหมายและปีก่อนหน้า
๒. ผลการประเมิน Readiness Assessment และระดับความพร้อมปัจจุบัน
๓. เหตุการณ์ด้านความปลอดภัยที่เกิดขึ้น มาตรการแก้ไข และแผนป้องกัน
๔. สถานะการปฏิบัติตามกฎหมาย (เช่น PDPA, พ.ร.บ. รัฐบาลดิจิทัล ฯลฯ)
๕. ผลการตรวจสอบ (Audit Result) และประเด็นที่ต้องปรับปรุง
๖. ความต้องการและข้อเสนอแนะของผู้มีส่วนได้เสีย
๗. แผนพัฒนาธรรมาภิบาลข้อมูลสำหรับปีถัดไป พร้อมงบประมาณและทรัพยากรที่ต้องการ

๕.๓.๓ กระบวนการปรับปรุงอย่างต่อเนื่อง

1. รวบรวมข้อมูลที่เกี่ยวข้องกับการดำเนินงาน เช่น ผลการติดตาม KPI ผลการตรวจสอบคุณภาพข้อมูล ข้อร้องเรียนจากผู้ใช้งาน และข้อเสนอแนะจากหน่วยงานที่เกี่ยวข้อง เพื่อนำมาใช้เป็นข้อมูลประกอบการปรับปรุง
2. วิเคราะห์หาสาเหตุของปัญหาที่พบ โดยเฉพาะปัญหาที่เกิดซ้ำหรือส่งผลกระทบต่อการทำงาน เพื่อหาสาเหตุที่แท้จริง ไม่ใช่เพียงแก้ไขเฉพาะอาการของปัญหา
3. กำหนดมาตรการแก้ไข โดยจัดทำแผนการแก้ไขปัญหา โดยระบุแนวทางดำเนินการ ผู้รับผิดชอบ ระยะเวลา และผลลัพธ์ที่คาดหวัง เพื่อให้การแก้ไขมีทิศทางชัดเจนและติดตามได้
4. ผู้รับผิดชอบดำเนินการแก้ไขตามแผนที่กำหนดไว้ พร้อมประสานงานกับหน่วยงานที่เกี่ยวข้อง เพื่อให้การปรับปรุงเกิดขึ้นจริงและไม่กระทบต่อการให้บริการข้อมูล
5. ติดตามผลหลังการปรับปรุง โดยวัดผลจาก KPI และผลการตรวจสอบที่เกี่ยวข้อง เพื่อประเมินว่ามาตรการแก้ไขช่วยลดปัญหาและยกระดับคุณภาพการดำเนินงานได้จริงหรือไม่
6. บันทึกบทเรียนจากการดำเนินงาน ปัญหาที่พบ แนวทางแก้ไข และข้อควรปรับปรุง เพื่อนำไปพัฒนานโยบาย แนวปฏิบัติ หรือกระบวนการทำงานให้มีประสิทธิภาพมากขึ้นในรอบถัดไป

ภาคผนวก

นโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูล

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ (กพร.)

ภาคผนวก	หัวข้อ
ก	ร่างคำสั่งแต่งตั้งคณะกรรมการธรรมาภิบาลข้อมูล กพร.
ข	แบบฟอร์มมาตรฐานคำอธิบายชุดข้อมูล (Metadata Template — DGA ๑๔ Fields)
ค	แม่แบบข้อตกลงการแบ่งปันข้อมูล (Data Sharing Agreement — DSA)
ง	แม่แบบบันทึกรายการกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (RoPA Form)
จ	หลักเกณฑ์และตารางการจัดชั้นความลับข้อมูล (Data Classification Matrix)

เวอร์ชัน ๑.๐ | ปีงบประมาณ ๒๕๖๘

จัดทำเพื่อการตรวจประเมินระดับความพร้อมรัฐบาลดิจิทัล (TRIS) ประจำปี ๒๕๖๙

ภาคผนวก ก
คำสั่ง แต่งตั้งคณะกรรมการธรรมาภิบาลข้อมูล คุ้มครองข้อมูลส่วนบุคคลและรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

Order: Appointment of Data Governance Council, DPIM

คำสั่งกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่
ที่ ๓๗๗/๒๕๖๘
เรื่อง แต่งตั้งคณะกรรมการธรรมาภิบาลข้อมูล คุ้มครองข้อมูลส่วนบุคคล
และรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

เพื่อให้การปฏิบัติงานของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ เป็นไปด้วยความเรียบร้อย เหมาะสม สอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกาศ นโยบายที่เกี่ยวข้อง และภารกิจหน้าที่ตามโครงสร้างของหน่วยงาน

อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๕) พ.ศ. ๒๕๔๕ จึงแต่งตั้งคณะกรรมการธรรมาภิบาลข้อมูล คุ้มครองข้อมูลส่วนบุคคล และรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ โดยมีองค์ประกอบและอำนาจหน้าที่ ดังนี้

องค์ประกอบ

๑. อธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่	ประธานกรรมการ
๒. รองอธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ (ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO))	รองประธานกรรมการ
๓. เลขานุการกรม	กรรมการ
๔. ผู้อำนวยการกองทุกกอง	กรรมการ
๕. ผู้อำนวยการกลุ่มตรวจสอบภายใน	กรรมการ
๖. ผู้อำนวยการสำนักงานอุตสาหกรรมพื้นฐานและการเหมืองแร่เขต ๑-๘	กรรมการ
๗. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	กรรมการและเลขานุการ
๘. หัวหน้ากลุ่มสถิติและพัฒนาข้อมูล ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	กรรมการและ ผู้ช่วยเลขานุการ
๙. หัวหน้ากลุ่มพัฒนาระบบเครือข่ายและการสื่อสาร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	กรรมการและ ผู้ช่วยเลขานุการ

อำนาจหน้าที่

๑. กำหนดและปรับปรุงนโยบาย แนวปฏิบัติ มาตรการ และกรอบการดำเนินงาน รวมถึงตรวจสอบและกำกับดูแลการดำเนินการ ด้านธรรมาภิบาลข้อมูลภาครัฐของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ให้สอดคล้องกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

๒. กำหนดและปรับปรุงนโยบาย และแนวปฏิบัติ รวมถึงตรวจสอบและกำกับดูแลการดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๓. กำหนดและปรับปรุงนโยบาย แนวปฏิบัติ และกรอบมาตรฐาน รวมถึงตรวจสอบและกำกับดูแลการดำเนินการ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ให้สอดคล้องกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. แต่งตั้งคณะทำงาน เพื่อสนับสนุนการดำเนินงานด้านต่าง ๆ ตามที่คณะกรรมการมอบหมาย

๕. ปฏิบัติหน้าที่อื่นใดที่เกี่ยวข้องกับการดำเนินการด้านธรรมาภิบาลข้อมูลภาครัฐ การคุ้มครองข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๓ พฤศจิกายน พ.ศ. ๒๕๖๘

(นายอดิทัต วะสีนนท์)
อธิบดีกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่