นโยบายธรรมาภิบาลข้อมูลภาครัฐจังหวัดสมุทรปราการ

Data Governance Policy Samut Prakan Province

จัดทำโดย: สำนักงานจังหวัดสมุทรปราการ

ปรับปรุงล่าสุด: พฤษภาคม 2569

คำนำ

ด้วยสำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) หรือ DGA ได้จัดทำกรอบการกำกับดูแลข้อมูล (Data Governance Framework) เวอร์ชัน ๑.๐ เมื่อปี พ.ศ. ๒๕๖๑ เพื่อเป็นแนวทางให้หน่วยงานภาครัฐนำไปปรับใช้ในการบริหารจัดการและกำกับดูแลข้อมูลอย่างมีประสิทธิภาพ โดยมีองค์ประกอบหลัก ๖ ด้าน ได้แก่ สภาพแวดล้อม การนิยามข้อมูล กฎเกณฑ์ข้อมูล โครงสร้าง กระบวนการ และการวัดผล

จังหวัดสมุทรปราการจึงได้จัดทำนโยบายธรรมาภิบาลข้อมูลภาครัฐฉบับนี้ โดยอ้างอิงกรอบ DGA Framework เป็นหลัก ผนวกกับฐานอำนาจตาม พ.ร.บ. ระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ มาตรา ๕๗ ประกอบ พ.ร.ฎ. การบริหารงานเชิงพื้นที่แบบบูรณาการ พ.ศ. ๒๕๖๕ เพื่อกำหนดกรอบการบริหารจัดการข้อมูลของจังหวัดให้สอดคล้องกับมาตรฐานภาครัฐและกฎหมายที่เกี่ยวข้อง โดยนโยบายนี้ครอบคลุมการกำหนดบทบาทหน้าที่ผู้มีส่วนได้ส่วนเสีย กระบวนการบริหารจัดการตลอดวงจรชีวิตข้อมูล ๖ ขั้นตอนตามมาตรฐาน DGA การควบคุมการเข้าถึง การรับประกันคุณภาพข้อมูล การจัดทำบัญชีข้อมูลและ Metadata รวมถึงกลไกการแบ่งปันและแลกเปลี่ยนข้อมูล

สารบัญ

หน้า

ส่วนที่ 1 วัตถุประสงค์ และฐานอำนาจทางกฎหมาย

1.1 วัตถุประสงค์

1) กำหนดกรอบการบริหารจัดการข้อมูลตามมาตรฐาน DGA Data Governance Framework เวอร์ชัน ๑.๐

2) ส่งเสริมให้ส่วนราชการใช้ข้อมูลในการตัดสินใจเชิงนโยบาย (Evidence-Based Policy)

3) คุ้มครองข้อมูลส่วนบุคคลและข้อมูลที่มีความอ่อนไหวตามกฎหมาย

4) สนับสนุนการพัฒนาและเชื่อมโยงฐานข้อมูลผ่านระบบแลกเปลี่ยนข้อมูลภาครัฐ (GDX)

5) ยกระดับคุณภาพข้อมูลตามมิติคุณภาพ ๖ ด้านของ DGA

1.2 ฐานอำนาจทางกฎหมายและมาตรฐานอ้างอิง

กฎหมาย/มาตรฐาน	สาระสำคัญ
กรอบ DGA Framework v1.0 (พ.ศ. ๒๕๖๑)	มาตรฐานหลักของ สพร. ว่าด้วยการบริหารจัดการข้อมูลภาครัฐ ๖ องค์ประกอบ
พ.ร.บ. ระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ (มาตรา ๕๗)	ผู้ว่าฯ มีอำนาจบริหาร บูรณาการ กำกับดูแลส่วนราชการ
พ.ร.ฎ. การบริหารงานเชิงพื้นที่แบบบูรณาการ พ.ศ. ๒๕๖๕	จังหวัดบูรณาการข้อมูล วิเคราะห์ แลกเปลี่ยนระหว่างส่วนราชการ
พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA)	หลักเกณฑ์การเก็บ ใช้ เปิดเผยข้อมูลส่วนบุคคล
พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒	หน่วยงานรัฐจัดทำ แลกเปลี่ยน และใช้ประโยชน์ข้อมูลดิจิทัล
พ.ร.บ. ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐	หลักการเปิดเผยข้อมูลราชการ มีข้อยกเว้นตามกฎหมาย
มาตรฐาน DCAT-AP และมาตรฐาน Metadata ของ สพร.	มาตรฐาน Metadata และ Data Catalog เชื่อมโยงกับ data.go.th

1.3 กรอบการกำกับดูแลข้อมูล (Data Governance Framework)

จังหวัดสมุทรปราการนำกรอบการกำกับดูแลข้อมูลของ สพร. (DGA Data Governance Framework v1.0) มาเป็นแนวทางหลัก ซึ่งประกอบด้วย ๖ องค์ประกอบสำคัญ ดังนี้

องค์ประกอบ	ความหมาย	หมวดอ้างอิงใน DGA Framework
๑. สภาพแวดล้อม (Environment)	กฎหมาย ระเบียบ นโยบาย และวัฒนธรรมองค์กร	หมวด ๑ และหมวด ๑๑
๒. การนิยามข้อมูล (Data Definition)	หมวดหมู่ข้อมูล Metadata บัญชีข้อมูล คลัง Metadata	หมวด ๕
๓. กฎเกณฑ์ข้อมูล (Data Rules)	นโยบายข้อมูลและมาตรฐานข้อมูล	หมวด ๖
๔. โครงสร้าง (Structure)	โครงสร้างบุคลากรและบทบาทหน้าที่	หมวด ๓
๕. กระบวนการ (Process)	กระบวนการกำกับดูแลตลอดวงจรชีวิต ๖ ขั้นตอน	หมวด ๔
๖. การวัดผล (Metrics)	การประเมินความพร้อม คุณภาพ และความมั่นคงปลอดภัย	หมวด ๗ และหมวด ๘

อ้างอิงตาม Appendix ข ของ DGA Framework — บทบาทและความรับผิดชอบของผู้มีส่วนได้ส่วนเสียกับข้อมูล

1.4 ขอบเขตการบังคับใช้

1) ส่วนราชการประจำจังหวัดทุกส่วนราชการ

2) อำเภอทุกอำเภอ

3) องค์กรปกครองส่วนท้องถิ่น หน่วยงานรัฐวิสาหกิจ และส่วนราชการสังกัดกระทรวงต่างๆ ที่เกี่ยวข้องกับการเชื่อมโยงข้อมูลกับจังหวัด

4) ผู้ประมวลผลข้อมูลและผู้ให้บริการภายนอก (Third-party Processors) ที่ได้รับมอบหมาย

ส่วนที่ 2 โครงสร้างและบทบาทหน้าที่ (Data Governance Structure)

2.1 ระดับนโยบาย — คณะกรรมการธรรมาภิบาลข้อมูลจังหวัด

องค์ประกอบ:

1) ผู้ว่าราชการจังหวัดเป็นประธาน
2) รองผู้ว่าราชการจังหวัดที่ได้รับมอบหมาย เป็นรองประธาน
3) หัวหน้าส่วนราชการ และผู้แทน อำเภอ และองค์กรปกครองส่วนท้องถิ่น เป็นกรรมการ
4) หัวหน้าสำนักงานจังหวัด และสถิติจังหวัด เป็นกรรมการและเลขานุการร่วม

บทบาทหน้าที่:

5) กำหนดนโยบาย ยุทธศาสตร์ และแผนปฏิบัติการด้านธรรมาภิบาลข้อมูล
6) อนุมัติมาตรฐานข้อมูล หลักเกณฑ์ชั้นความลับ และนโยบายเปิดเผยข้อมูล
7) กำกับดูแลและติดตามผลการดำเนินงานในภาพรวม
8) รายงานผลต่อกระทรวงมหาดไทยและ สพร. ตามที่กำหนด

2.2 ระดับบริหาร

รองผู้ว่าราชการจังหวัดที่ได้รับมอบหมาย ทำหน้าที่ Chief Data Officer (CDO) ของจังหวัด มีบทบาทหน้าที่ ดังนี้

1) บริหารและประสานงานด้านธรรมาภิบาลข้อมูลระดับจังหวัด
2) บริหาร Data Catalog กลาง ระบบ Metadata และ Data Quality
3) ประสานงานกับ สพร. ตามมาตรฐาน DGA
4) จัดทำรายงาน Data Governance Readiness Assessment ประจำปี

2.3 ระดับปฏิบัติ — ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders)

บทบาท	ผู้ดำรงตำแหน่ง	ระดับสิทธิ์	หน้าที่หลักตามวงจรชีวิตข้อมูล
Data Owner	หัวหน้าส่วนราชการ	สูงสุดในหน่วยงาน	รับผิดชอบชุดข้อมูล กำหนดชั้นความลับ อนุมัติการสร้าง/เปิดเผย/ทำลาย

Data Steward	ผู้รับผิดชอบงานสารสนเทศ/IT	L3–L4	จัดทำ Metadata ดูแลคุณภาพ บริหารสิทธิ์ รายงานต่อ CDO
Data Custodian	ผู้ดูแลระบบ / IT Admin	L3	ดูแลระบบจัดเก็บ ความปลอดภัย สำรอง และกู้คืนข้อมูล
Data User	เจ้าหน้าที่ผู้ใช้ข้อมูล	L1–L3	ใช้ข้อมูลตามสิทธิ์ รายงานปัญหา ปฏิบัติตามนโยบาย
Data Architect	ผู้เชี่ยวชาญ IT/ระบบสารสนเทศ	เฉพาะด้าน	ออกแบบสถาปัตยกรรมข้อมูล แบบจำลองข้อมูล และระบบบูรณาการ

ส่วนที่ 3 กระบวนการกำกับดูแลข้อมูล (Data Governance Process)

3.1 บทบาทตามวงจรชีวิตข้อมูล ๖ ขั้นตอน (ตามมาตรฐาน DGA)

ขั้นตอน (DGA)	ผู้รับผิดชอบหลัก	ผู้สนับสนุน	ผู้กำกับดูแล
๑. สร้าง (Create)	Data Owner, Steward	Data Custodian	CDO
๒. จัดเก็บ (Store)	Data Custodian	Data Steward	CDO
๓. ใช้ (Use)	Data User	Data Steward	Data Owner
๔. เผยแพร่ (Publish)	Data Owner	CDO, Steward	คณะกรรมการฯ
๕. จัดเก็บถาวร (Archive)	Data Custodian	Data Owner	CDO
๖. ทำลาย (Destroy)	Data Owner	Data Custodian	CDO

อ้างอิงตาม DGA Framework หมวด ๓.๕ — กระบวนการกำกับดูแลข้อมูล

3.2 ขั้นตอนที่ ๑ — การสร้างข้อมูล (Create)

การสร้างข้อมูลขึ้นมาใหม่ โดยบุคคลหรืออัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ รวมถึงการรับข้อมูลจากหน่วยงานอื่น ดำเนินการดังนี้

1) กำหนด "นิยามข้อมูล" (Data Definition) ก่อนการสร้างหรือรวบรวมทุกชุด
2) บันทึก Metadata ทันทีที่มีการสร้างชุดข้อมูลใหม่
3) การรวบรวมข้อมูลส่วนบุคคลต้องดำเนินการตาม พ.ร.บ. PDPA พ.ศ. ๒๕๖๒
4) ใช้รูปแบบข้อมูลมาตรฐานที่กำหนดโดยสำนักงานจังหวัดเพื่อให้เชื่อมโยงได้

3.3 ขั้นตอนที่ ๒ — การจัดเก็บข้อมูล (Store)

การจัดเก็บข้อมูลจากกระบวนการสร้างหรือรับจากหน่วยงานอื่น ให้มีระเบียบและง่ายต่อการใช้งาน ดำเนินการดังนี้

1) จัดเก็บในระบบที่รองรับมาตรฐาน ISO/IEC 27001 หรือเทียบเท่า
2) ข้อมูลระดับลับขึ้นไปต้องเข้ารหัสทั้ง At Rest และ In Transit
3) สำรองข้อมูลอย่างน้อย ๓ ชุดตามหลัก 3-2-1 Backup Rule
4) ระบบจัดเก็บต้องมีความพร้อมใช้งาน ≥ ๙๙.๕% ต่อปี สำหรับข้อมูลสำคัญ

3.4 ขั้นตอนที่ ๓ — การใช้ข้อมูล (Use)

การนำข้อมูลมาประมวลผล เช่น การถ่ายโอน การวิเคราะห์ การจัดทำรายงาน และการสำรองข้อมูล ดำเนินการดังนี้

1) การประมวลผลต้องเป็นไปตามวัตถุประสงค์ที่กำหนดใน Metadata

2) การใช้เพื่อวัตถุประสงค์อื่นต้องได้รับอนุมัติจาก Data Owner

3) การวิเคราะห์ข้อมูลขนาดใหญ่ต้องผ่าน Anonymization/Pseudonymization ก่อน

4) บันทึก Data Audit Log ทุกครั้งที่เข้าถึงข้อมูลระดับลับขึ้นไป

3.5 ขั้นตอนที่ ๔ — การเผยแพร่ข้อมูล (Publish)

การแชร์ การกระจาย การควบคุมการเข้าถึง การแลกเปลี่ยนระหว่างหน่วยงาน และการกำหนดเงื่อนไขการใช้งาน ดำเนินการดังนี้

1) การเปิดเผยต้องเป็นไปตาม พ.ร.บ. ข้อมูลข่าวสาร และ PDPA

2) ข้อมูล Open Data ต้องเผยแพร่บนระบบบัญชีข้อมูลจังหวัดสมุทรปราการ ภายใน ๓๐ วันหลังจัดทำ

3) ปกปิดข้อมูลส่วนบุคคลก่อนเผยแพร่ด้วย Data Masking

4) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานใช้ช่องทาง API

3.6 ขั้นตอนที่ ๕ — การจัดเก็บข้อมูลถาวร (Archive)

การคัดลอกข้อมูลที่มีช่วงอายุเกินช่วงใช้งาน เพื่อทำสำเนาสำหรับเก็บรักษาโดยไม่มีการลบหรือแก้ไข

1) กำหนดเกณฑ์การย้ายข้อมูลไป Archive ตามอายุการใช้งานและกฎหมาย

2) ข้อมูลที่มีคุณค่าทางประวัติศาสตร์ให้โอนไปเก็บถาวรก่อนทำลาย

3) บันทึกทะเบียนข้อมูลถาวรพร้อม Metadata เพื่อให้เรียกคืนได้

3.7 ขั้นตอนที่ ๖ — การทำลายข้อมูล (Destroy)

การทำลายข้อมูลที่สิ้นสุดระยะเวลาหรือสิ้นสุดวัตถุประสงค์การใช้งาน

1) ใช้วิธีมาตรฐาน Secure Erasure / Physical Destruction ตาม NIST SP 800-88

2) จัดทำบันทึกการทำลายลงนามโดย Data Owner และ Data Custodian

3) ข้อมูลส่วนบุคคลที่สิ้นสุดวัตถุประสงค์ต้องทำลายทันที เว้นแต่มีกฎหมายกำหนด

ส่วนที่ 4 การนิยามข้อมูล (Data Definition)

อ้างอิงตาม DGA Framework หมวด ๓.๒

4.1 หมวดหมู่ข้อมูลและการจำแนกชั้นความลับ

ระดับ	ชั้นความลับ	ลักษณะข้อมูล	ตัวอย่าง	มาตรการ
๑	ข้อมูลเปิด (Open Data)	เปิดเผยต่อสาธารณะได้ไม่มีข้อจำกัด	สถิติจังหวัด งบประมาณรายจ่าย	เผยแพร่ data.go.th ภายใน ๓๐ วัน
๒	ข้อมูลภายใน (Internal)	ใช้งานภายในหน่วยงานรัฐ	รายงานประชุม แผนงาน ร้องเรียน	ยืนยันตัวตน บันทึก Audit Log
๓	ข้อมูลส่วนบุคคล (Personal)	ระบุตัวบุคคลได้ คุ้มครองตาม PDPA	ทะเบียนราษฎร์ ข้อมูลผู้ร้อง	เข้ารหัส Data Masking 2FA
๔	ข้อมูลลับ (Confidential)	อ่อนไหว หากเปิดเผยกระทบต่อบุคคล/องค์กร	ข้อมูลสุขภาพ ภาษี คดีความ	เข้ารหัสระดับสูง เฉพาะผู้ได้รับอนุญาต
๕	ข้อมูลลับมาก (Restricted)	ด้านความมั่นคงและยุทธศาสตร์รัฐ	แผนรับมือภัยพิบัติ ความมั่นคงพื้นที่	เฉพาะผู้ได้รับมอบหมายเป็นการเฉพาะ

4.2 Metadata — มาตรฐานการจัดทำ

อ้างอิง Appendix ก ของ DGA Framework ประกอบมาตรฐาน DCAT-AP ของ สพร.

องค์ประกอบ Metadata	คำอธิบาย	บังคับ	แนะนำ
ชื่อชุดข้อมูล (Title)	ชื่อภาษาไทยและอังกฤษที่ชัดเจน	✓	
คำอธิบาย (Description)	เนื้อหา วัตถุประสงค์ และขอบเขต	✓	
หมวดหมู่ (Category)	จำแนกตาม ๑๗ หมวดมาตรฐาน data.go.th	✓	
ชั้นความลับ (Classification)	ระดับ ๑–๕ ตามนโยบายนี้	✓	
เจ้าของข้อมูล (Data Owner)	ชื่อหน่วยงาน ผู้รับผิดชอบ เบอร์ติดต่อ	✓	
วันที่จัดทำ/ปรับปรุง	วันจัดทำครั้งแรกและอัปเดตล่าสุด	✓	
ความถี่การปรับปรุง (Frequency)	รายวัน/สัปดาห์/เดือน/ปี/ไม่ระบุ	✓	
รูปแบบข้อมูล (Format)	CSV, JSON, XML, API, Excel, PDF	✓	

สิทธิ์การใช้งาน (License)	Open Government License, CC-BY ฯลฯ	✓	
สถานะข้อมูล (Status)	Active / Inactive / Archived / Destroyed	✓	
คำสำคัญ (Keywords)	คำสำคัญสำหรับการค้นหา		✓
พื้นที่ครอบคลุม (Spatial Coverage)	ระดับจังหวัด/อำเภอ/ตำบล/พิกัด GIS		✓
ช่วงเวลา (Temporal Coverage)	ปีงบประมาณ/ปีปฏิทินที่ครอบคลุม		✓
Data Lineage	ที่มา กระบวนการสร้าง และการแปลงข้อมูล		✓

4.3 บัญชีข้อมูล (Data Catalog) และคลัง Metadata

อ้างอิงตาม DGA Framework หมวด ๓.๒.๓ และ ๓.๒.๔

4.3.1 Data Catalog สาธารณะ (Public Catalog)

1) เผยแพร่บนระบบบัญชีข้อมูลจังหวัดสมุทรปราการและเชื่อมโยงกับ data.go.th
2) ครอบคลุมชุดข้อมูล Open Data ระดับ ๑ ทั้งหมด
3) ปรับปรุงทุกไตรมาส หรือทุกครั้งที่มีชุดข้อมูลใหม่
4) รองรับ API สำหรับเชื่อมโยงกับระบบภายนอก

4.3.2 Data Catalog ภายใน / คลัง Metadata (Internal Catalog / Metadata Repository)

1) ระบบปิดเฉพาะเจ้าหน้าที่ ครอบคลุมข้อมูลระดับ ๑–๕
2) บันทึก Data Lineage และประวัติการเปลี่ยนแปลง Metadata
3) เชื่อมโยงกับระบบ Data Request Management
4) ค้นหาตามหมวดหมู่ ชั้นความลับ และหน่วยงานเจ้าของ

4.4 บัญชีข้อมูลหลักของจังหวัด (Provincial Master Data Inventory)

ทุกส่วนราชการส่งบัญชีข้อมูลที่รับผิดชอบปีละ ๑ ครั้ง จำแนกเป็น ๑๐ กลุ่มข้อมูลหลัก ดังนี้

1) ด้านประชากรและทะเบียนราษฎร์ (ทร./ปค.)
2) ด้านเศรษฐกิจ การค้า และอุตสาหกรรม (พณ./อก./ศุลกากร)
3) ด้านทรัพยากรธรรมชาติและสิ่งแวดล้อม (ทส.)

4) ด้านสาธารณสุขและสังคม (สธ./พม.)

5) ด้านการศึกษา (ศธ.)

6) ด้านโครงสร้างพื้นฐานและการขนส่ง (คค.)

7) ด้านความมั่นคงและการรักษาความสงบ (ตช./กห.)

8) ด้านงบประมาณและการคลัง (กค.)

9) ด้านการเกษตร (กษ.)

10) ด้านภัยพิบัติและการบริหารในภาวะฉุกเฉิน (มท./ปภ.)

ส่วนที่ 5 กฎเกณฑ์และนโยบายข้อมูล (Data Rules & Policies)

อ้างอิงตาม DGA Framework หมวด ๓.๓ ประกอบ Appendix ค และ ง

5.1 นโยบายการควบคุมสิทธิ์การเข้าถึงข้อมูล (Access Control Policy)

5.1.1 หลักการพื้นฐาน

1) Least Privilege Principle — กำหนดสิทธิ์ขั้นต่ำที่จำเป็นต่อการปฏิบัติงาน
2) Need-to-Know Basis — เข้าถึงเฉพาะที่จำเป็นต่อหน้าที่
3) Separation of Duties — แยกสิทธิ์การสร้าง อนุมัติ และตรวจสอบออกจากกัน
4) Zero Trust Architecture — ตรวจสอบและยืนยันตัวตนทุกครั้งก่อนอนุญาต

5.1.2 ระดับสิทธิ์การเข้าถึง

ระดับสิทธิ์	กลุ่มผู้ใช้	สิทธิ์การดำเนินการ	ข้อมูลที่เข้าถึงได้
L1 - Public	ประชาชนทั่วไป	อ่านอย่างเดียว	ข้อมูลระดับ ๑ (Open Data)
L2 - Staff	เจ้าหน้าที่ภายใน	อ่าน + ส่งออก	ข้อมูลระดับ ๑–๒
L3 - Officer	เจ้าหน้าที่ผู้รับผิดชอบ	อ่าน แก้ไข ส่งออก	ข้อมูลระดับ ๑–๓ ตามขอบเขต
L4 - Steward	Data Steward / ผู้ดูแลระบบ	อ่าน แก้ไข ลบ จัดการสิทธิ์	ข้อมูลระดับ ๑–๔ ในขอบเขตที่รับผิดชอบ
L5 - Owner/CDO	Data Owner / CDO	สิทธิ์เต็ม รวมถึงการทำลาย	ข้อมูลทุกระดับในขอบเขตรับผิดชอบ

5.1.3 กระบวนการขอและอนุมัติสิทธิ์

1) ผู้ใช้ยื่นคำขอผ่านระบบ Data Request Management พร้อมระบุเหตุผล
2) หัวหน้าหน่วยงานตรวจสอบและรับรองความจำเป็น
3) Data Steward ของหน่วยงานเจ้าของพิจารณาอนุมัติ/ปฏิเสธ
4) ข้อมูลระดับ ๔–๕ ต้องผ่านการอนุมัติจาก CDO เพิ่มเติม
5) กำหนดสิทธิ์และบันทึกในระบบภายใน ๓ วันทำการ
6) ทบทวนสิทธิ์ทุก ๖ เดือน หรือเมื่อเปลี่ยนตำแหน่ง/โอนย้าย

5.1.4 มาตรการรักษาความปลอดภัย

1) Two-Factor Authentication (2FA) บังคับสำหรับข้อมูลระดับ ๓ ขึ้นไป

2) Single Sign-On (SSO) เชื่อมกับระบบบัญชีผู้ใช้ส่วนกลาง

3) บันทึก Audit Log ทุกรายการ เก็บไม่น้อยกว่า ๒ ปี

4) ยกเลิกสิทธิ์ทันทีเมื่อเจ้าหน้าที่ออกหรือย้าย

5) ห้ามส่งข้อมูลระดับ ๓ ขึ้นไปผ่านช่องทางที่ไม่เข้ารหัส

5.2 มาตรฐานข้อมูล (Data Standards)

ต้องมีมาตรฐานชั้นพื้นฐาน ดังนี้

1) Metadata มาตรฐาน DCAT-AP และมาตรฐาน สพร.

2) รหัสอ้างอิงมาตรฐานร่วม เช่น รหัสจังหวัด/อำเภอ ตาม ISO 3166

3) รูปแบบวันที่ ISO 8601 (YYYY-MM-DD)

4) การเข้ารหัสอักขระ UTF-8

5) API มาตรฐาน RESTful ตามแนวทางของ สพร.

5.3 นโยบายการแลกเปลี่ยนข้อมูล

อ้างอิง DGA Appendix ค

1) ใช้ช่องทาง API ของระบบบัญชีข้อมูลจังหวัดสมุทรปราการสำหรับแลกเปลี่ยนระหว่างหน่วย

2) ข้อมูลระดับ ๒ ขึ้นไปต้องมี Data Sharing Agreement (DSA) ระบุวัตถุประสงค์ ระยะเวลา และเงื่อนไข

3) ห้ามส่งต่อข้อมูลที่ได้รับจากหน่วยงานอื่นไปยังบุคคลที่สาม โดยไม่ได้รับอนุญาต

4) บันทึกรายการแลกเปลี่ยนข้อมูลทุกครั้งใน Data Audit Log

5.4 นโยบายการเปิดเผยข้อมูล

อ้างอิง DGA Appendix ง

1) ยึดหลัก "Open by Default" — ข้อมูลสาธารณะเปิดเผยโดยค่าเริ่มต้น การปฏิเสธต้องมีเหตุผลตามกฎหมาย

2) Open Data ต้องอยู่ในรูปแบบ machine-readable และมี API รองรับ

3) ประชาชนยื่นขอข้อมูลตาม พ.ร.บ. ข้อมูลข่าวสาร ต้องได้รับคำตอบภายใน ๑๕ วัน

4) กรณีปฏิเสธ ต้องแจ้งเหตุผลและสิทธิ์การอุทธรณ์

ส่วนที่ 6 มาตรการประเมินคุณภาพข้อมูล (Data Quality Assessment)

อ้างอิงตาม DGA Framework หมวด ๓.๖.๒

6.1 มิติคุณภาพข้อมูล ๖ ด้าน (ตามมาตรฐาน DGA)

มิติ	ความหมาย	เกณฑ์เป้าหมาย	เครื่องมือประเมิน
ความถูกต้อง (Accuracy)	ข้อมูลตรงกับความเป็นจริง	≥ ๙๕%	Data Validation Rules
ความสมบูรณ์ (Completeness)	ข้อมูลครบถ้วนตามโครงสร้าง	≥ ๙๕%	Null/Missing Check
ความทันสมัย (Timeliness)	ปรับปรุงตามรอบที่กำหนด	ตามรอบ	Update Timestamp Monitor
ความสอดคล้อง (Consistency)	ค่าตรงกันในทุกระบบ	≥ ๙๘%	Cross-system Reconciliation
ความไม่ซ้ำซ้อน (Uniqueness)	ไม่มีระเบียนซ้ำกัน	< ๐.๕%	Duplicate Detection Tool
ความถูกรูปแบบ (Conformity)	เป็นไปตามมาตรฐานที่กำหนด	๑๐๐%	Schema / Format Validator

6.2 กระบวนการรับรองคุณภาพข้อมูล

1) Data Steward ตรวจสอบคุณภาพรายเดือนตามมิติที่กำหนด
2) บันทึกผลใน Data Quality Dashboard
3) ชุดข้อมูลที่ไม่ผ่านเกณฑ์ต้องปรับปรุงและรายงานสาเหตุภายใน ๑๕ วัน
4) CDO สรุปผลรายไตรมาส เสนอคณะกรรมการธรรมาภิบาลข้อมูล
5) ประเมินแนวโน้มเชิงสถิติรายปี เพื่อวางแผนพัฒนาระยะยาว

6.3 เครื่องมือและระบบประเมินคุณภาพ

1) Data Quality Dashboard — แสดงสถานะคุณภาพแบบ Real-time
2) Automated Data Validation — ตรวจสอบอัตโนมัติเมื่อนำเข้าหรืออัปเดตข้อมูล
3) Data Profiling Tool — วิเคราะห์โครงสร้างและสถิติของชุดข้อมูลรายเดือน
4) Annual Data Quality Assessment — ประเมินโดยคณะทำงานรายปี

ส่วนที่ 7 การวัดและประเมินผลธรรมาภิบาลข้อมูล (Data Governance Metrics)

อ้างอิงตาม DGA Framework หมวด ๓.๖

7.1 การประเมินความพร้อมธรรมาภิบาลข้อมูล (Data Governance Readiness Assessment)

อ้างอิง DGA Framework ตารางที่ ๑๖ ระดับความพร้อมของการกำกับดูแลข้อมูล

ระดับ	ชื่อระดับ	ลักษณะ	เป้าหมายจังหวัด
๑	เริ่มต้น (Initial)	ไม่มีกระบวนการอย่างเป็นทางการ	ผ่านแล้ว (ปีงบ ๒๕๖๗)
๒	พัฒนา (Developing)	มีนโยบายบางส่วน ยังไม่ครบถ้วน	เป้าหมาย ปีงบ ๒๕๖๘
๓	กำหนด (Defined)	มีนโยบาย กระบวนการ บทบาทชัดเจน	เป้าหมาย ปีงบ ๒๕๖๙
๔	วัดได้ (Managed)	มีการวัด KPI และปรับปรุงตามผล	เป้าหมาย ปีงบ ๒๕๗๐
๕	เหมาะสมที่สุด (Optimizing)	ปรับปรุงต่อเนื่อง นวัตกรรม เป็นแบบอย่าง	เป้าหมายระยะยาว

7.2 ตัวชี้วัดสำคัญ (KPIs)

ตัวชี้วัด	เกณฑ์เป้าหมาย	รอบประเมิน	ผู้รับผิดชอบ
ชุดข้อมูล Open Data บน data.go.th	เพิ่มขึ้น ≥ ๒๐% ต่อปี	รายปี	CDO / สจ.
คะแนนคุณภาพข้อมูลเฉลี่ย	≥ ๘๕ คะแนน	รายไตรมาส	Data Steward
ร้อยละหน่วยงานที่มี Data Steward	๑๐๐%	รายปี	CDO
เวลาเฉลี่ยอนุมัติคำขอเข้าถึงข้อมูล	≤ ๓ วันทำการ	รายเดือน	Data Steward
เหตุการณ์ละเมิดข้อมูล (Data Breach)	= ๐ เหตุการณ์	รายปี	Data Custodian / CDO
ร้อยละชุดข้อมูลที่มี Metadata ครบ	≥ ๙๐%	รายไตรมาส	Steward / CDO
ชุดข้อมูลแบ่งปัน G2G ผ่าน GDX	เพิ่มขึ้น ≥ ๑๕% ต่อปี	รายปี	CDO
เจ้าหน้าที่ผ่านอบรม Data Governance	≥ ๘๐% ของกลุ่มเป้าหมาย	รายปี	สำนักงานจังหวัด

ระดับความพร้อม DGA (Readiness Level)	ระดับ ๒ (ปีงบ ๖๘) ⟶ ๓ (ปีงบ ๖๙)	รายปี	CDO / คณะกรรมการ

7.3 การประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security Assessment)

อ้างอิงตาม DGA Framework หมวด ๓.๖.๓

1) การประเมินการควบคุมการเข้าถึง (Access Control Assessment)
2) การทดสอบการเจาะระบบ (Penetration Testing) สำหรับระบบจัดเก็บข้อมูลสำคัญ
3) การตรวจสอบ Audit Log และรายงานความผิดปกติ
4) การประเมินความเสี่ยงด้านข้อมูล (Data Risk Assessment)

7.4 กลไกติดตามและรายงานผล

รายเดือน: Data Steward ส่งรายงานสถานะผ่านระบบออนไลน์

1) รายไตรมาส: CDO รวบรวมวิเคราะห์ รายงานต่อคณะกรรมการธรรมาภิบาลข้อมูล
2) รายปี: จัดทำรายงานธรรมาภิบาลข้อมูลประจำปี เผยแพร่บนเว็บไซต์จังหวัด และส่งให้ สพร.
3) ทุก ๒ ปี: ทบทวนนโยบาย หรือเมื่อมีการเปลี่ยนแปลงกฎหมายที่เกี่ยวข้อง

ส่วนที่ 8 นโยบายและแผนการแบ่งปันข้อมูล (Data Sharing Policy)

อ้างอิง DGA Appendix ค และ ง — หลักการ "เปิดข้อมูลสูงสุด ปกป้องข้อมูลจำเป็น"

8.1 รูปแบบการแบ่งปันข้อมูล

รูปแบบ	กลุ่มเป้าหมาย	ช่องทาง	เงื่อนไข
Open Data	ประชาชน นักวิจัย สื่อมวลชน	data.go.th / เว็บจังหวัด / API	ไม่มีเงื่อนไข ใช้ Open Government License
G2G (via GDX)	หน่วยงานรัฐ	Government Data Exchange (GDX)	DSA + บันทึก Audit Log
G2B	ภาคเอกชนที่ได้รับอนุญาต	API พร้อม API Key	สัญญาการใช้ข้อมูล + NDA + จำกัดวัตถุประสงค์
G2C	ประชาชนที่เกี่ยวข้อง	บริการออนไลน์ / ทางรัฐ	ยืนยันตัวตน + จำกัดเฉพาะข้อมูลของตนเอง
Academic/Research	สถาบันการศึกษา นักวิจัย	Data Sandbox / Anonymized Data	โครงการที่ได้รับอนุมัติ + Ethics Committee

8.2 ข้อตกลงการแลกเปลี่ยนข้อมูล (Data Sharing Agreement: DSA)

การแบ่งปันข้อมูลระดับ ๒ ขึ้นไปทุกกรณีต้องมี DSA ระบุ

1) วัตถุประสงค์และขอบเขตที่อนุญาต
2) ระยะเวลาการใช้งานและเงื่อนไขการต่ออายุ
3) ข้อห้าม (ห้ามขาย ห้ามส่งต่อ ห้ามใช้นอกวัตถุประสงค์)
4) มาตรการรักษาความปลอดภัยที่ผู้รับต้องปฏิบัติ
5) สิทธิ์ในการตรวจสอบและเพิกถอนการเข้าถึง
6) บทกำหนดโทษกรณีละเมิด

8.3 แผนปฏิบัติการแบ่งปันข้อมูล ๓ ระยะ

8.3.1 ระยะที่ ๑ (ปีงบประมาณ ๒๕๖๙): วางรากฐาน

1) จัดทำ Data Catalog และ Metadata มาตรฐานบัญชีข้อมูลหลักให้ครบถ้วน

2) เปิดเผย Open Data สำคัญ ≥ ๕๐ ชุดบนระบบบัญชีข้อมูลจังหวัด

3) พัฒนาระบบ Data Request Management และ Access Control

4) อบรมเจ้าหน้าที่ด้าน Data Governance

8.3.2 ระยะที่ ๒ (ปีงบประมาณ ๒๕๗๐): พัฒนาระบบ

1) พัฒนา API สำหรับชุดข้อมูลสำคัญ ≥ ๒๐ ชุด

2) เปิดเผย Open Data เพิ่มเติม ≥ ๕๐ ชุด

3) พัฒนา Data Quality Dashboard แบบ Real-time

8.3.3 ระยะที่ ๓ (ปีงบประมาณ ๒๕๗๑): ยกระดับสู่ความยั่งยืน

1) บรรลุระดับความพร้อม DGA ระดับ ๔ (Managed)

2) เปิดชุดข้อมูลสำหรับ AI/ML พร้อม Anonymization

3) ร่วมมือภาคเอกชนสร้างนวัตกรรมจากข้อมูลภาครัฐ (Data-driven Innovation)

ภาคผนวก: ตารางอ้างอิง DGA Framework กับนโยบายจังหวัดสมุทรปราการ

องค์ประกอบ DGA Framework	หมวดอ้างอิง DGA	การนำใช้ในนโยบายจังหวัดสมุทรปราการ
สภาพแวดล้อม — กฎหมาย ระเบียบ นโยบาย	บทที่ ๓.๑	ส่วนที่ ๑ (§1.5): กฎหมายอ้างอิง ๗ ฉบับ รวม DGA Framework, PDPA, พ.ร.บ. ข้อมูลข่าวสาร
การนิยามข้อมูล — หมวดหมู่ Metadata Data Catalog	บทที่ ๓.๒	ส่วนที่ ๔: หมวดหมู่ข้อมูล ๕ ระดับ, Metadata ๑๔ องค์ประกอบ, Data Catalog ๒ ระดับ
กฎเกณฑ์ — นโยบาย + มาตรฐาน (Appendix ค ง)	บทที่ ๓.๓	ส่วนที่ ๕: Access Control 5 ระดับ, มาตรฐาน DCAT-AP, DSA, Open by Default
โครงสร้าง — Roles & Responsibilities (Appendix ข)	บทที่ ๓.๔	ส่วนที่ ๒: Data Owner, Steward, Custodian, User, Architect ครบ ๕ บทบาท
กระบวนการ — Data Lifecycle 6 ขั้นตอน	บทที่ ๓.๕	ส่วนที่ ๓: Create⟶Store⟶Use⟶Publish⟶Archive⟶Destroy ครบ ๖ ขั้นตอน
การวัดผล — Readiness, Quality, Security Assessment	บทที่ ๓.๖	หมวด ๗ (คุณภาพ 6 มิติ) + หมวด ๘ (Readiness 5 ระดับ, KPI 9 ตัว, Security Assessment)

เอกสารนี้จัดทำขึ้นตามกรอบการกำกับดูแลข้อมูล (Data Governance Framework) เวอร์ชัน ๑.๐ สำนักงานพัฒนารัฐบาลดิจิทัล (สพร./DGA) พ.ศ. ๒๕๖๑