



คู่มือบริหารจัดการข้อมูลที่ดี

**(DATA GOVERNANCE HANDBOOK)**

โครงการจัดจ้างที่ปรึกษาวิเคราะห์และจัดทำแนวทงนโยบาย  
ธรรมาภิบาลข้อมูลภาครัฐเพื่อนำไปสู่การพัฒนาชุดข้อมูลเปิด  
ของกรมประชาสัมพันธ์

MAY 2023

PREPARED BY



THAMMASAT UNIVERSITY  
RESEARCH AND CONSULTANCY INSTITUTE  
สถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

วัตถุประสงค์	1
ขอบเขต	1
อ้างอิง	1
คำจำกัดความและความหมาย	2
ภาพรวมของมาตรฐานเรื่อง การกำกับดูแลข้อมูล (Data Governance Standard) ของกรมประชาสัมพันธ์	3
1. การกำกับดูแลข้อมูล	4
1.1 การจัดโครงสร้างองค์กรในการกำกับดูแลข้อมูล	4
1.2 นโยบายการกำกับดูแลข้อมูล	9
2. การบริหารจัดการข้อมูล (Data Management)	14
2.1 วงจรชีวิตของข้อมูล (Data Life Cycle)	14
2.2 การบริหารจัดการคำอธิบายชุดข้อมูล (Metadata Management)	15
2.3 การบริหารจัดการคุณภาพข้อมูล (Data Quality Management)	16
2.4 การบริหารจัดการความเสี่ยงด้านข้อมูล (Data Risk Management)	18
2.5 การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)	20
2.6 การรักษาความเป็นส่วนตัวของข้อมูล (Data Privacy)	21
3. แนวทางการประเมินระดับการกำกับดูแลข้อมูล (Data Governance Maturity Assessment)	22
3.1 แนวทางการประเมินระดับการกำกับดูแลข้อมูล (Data Governance Maturity Assessment)	22
3.2 องค์ประกอบและมิติของการประเมินระดับความพร้อมของการกำกับดูแลข้อมูล	23
4. การสร้าง การจัดเก็บรักษา การทำลาย และการควบคุมคุณภาพข้อมูล	26
4.1 แนวปฏิบัติการสร้างข้อมูล	26
4.2 แนวปฏิบัติการจัดเก็บข้อมูล	26
4.3 แนวปฏิบัติการทำลายข้อมูล (Data Destruction)	27
4.4 แนวปฏิบัติการควบคุมคุณภาพข้อมูล (Data Quality)	28
5. การประมวลผลและการใช้ข้อมูล	35
5.1 แนวปฏิบัติการประมวลผลข้อมูล	35
5.2 แนวปฏิบัติการใช้ข้อมูล	35
6. การเปิดเผยข้อมูล/การเชื่อมโยงข้อมูลและการรักษาความลับ	36

## วัตถุประสงค์

1. เพื่อกำหนดนโยบายให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับกรมประชาสัมพันธ์ตระหนักถึงความสำคัญของธรรมาภิบาลข้อมูล
2. เพื่อเป็นแนวทางในการควบคุม และตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การใช้ การเผยแพร่ จนถึงการทำลาย
3. เพื่อให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับกรมประชาสัมพันธ์ มีแนวทางในการดำเนินงานที่เกี่ยวข้องกับข้อมูล โดยครอบคลุมประเด็นต่อไปนี้
  - คุณภาพข้อมูล (Data Quality)
  - ความพร้อมใช้งานของข้อมูล (Data Availability)
  - การใช้งานข้อมูล (Data Usability)
  - ความถูกต้องของข้อมูล (Data Integrity)
  - ความปลอดภัยของข้อมูล (Data Security)



## ขอบเขต

ใช้สำหรับการบริการจัดการข้อมูลสำหรับกรมประชาสัมพันธ์ และหน่วยงานที่เกี่ยวข้อง ให้ข้อมูลดังกล่าวพร้อมใช้งาน ถูกต้อง ปลอดภัย และเพื่อสามารถนำข้อมูลมาใช้งานได้มีประสิทธิภาพมากที่สุด ทั้งในแง่ของใช้ประโยชน์ภายในองค์กร และรองรับความต้องการของประชาชน

## อ้างอิง

(References outside the company document system, such as the law, regulation, etc.)

- DAMA – DMBOK (หัวข้อ Data Management)
- ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

## คำจำกัดความและความหมาย

การกำกับดูแลข้อมูล  
(Data Governance)

แนวคิดและกระบวนการสำหรับการจัดการข้อมูลในการทำให้มั่นใจว่าข้อมูลจะมีคุณภาพสูงตลอด Lifecycle

การบริหารจัดการข้อมูล  
(Data Management)

การควบคุมข้อมูล ไม่ว่าจะเป็นการเข้าถึง การเก็บรักษา ไปจนถึงการทำลายข้อมูลตามวงจรชีวิต (Data Life Cycle)

คำอธิบายชุดข้อมูล  
(Metadata)

ข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจและเชิงเทคโนโลยีสารสนเทศ ให้รายละเอียดถึงกฎ ข้อจำกัดของข้อมูล และโครงสร้างของข้อมูล ช่วยให้องค์กรสามารถเข้าใจข้อมูล ระบบ และขั้นตอนการทำงานได้ดียิ่งขึ้น

การบริหารจัดการคำอธิบายชุดข้อมูล  
(Metadata Management)

กระบวนการที่เกี่ยวข้องกับการบริหารจัดการหรือควบคุมคำอธิบายชุดข้อมูล เพื่อให้สามารถมั่นใจว่าคำอธิบายชุดข้อมูลสามารถมีการเข้าถึง แบ่งปัน เชื่อมโยง วิเคราะห์ และบูรณาการ ให้เกิดประสิทธิผลทั่วทั้งองค์กร

คุณภาพข้อมูล  
(Data Quality)

ข้อมูลที่ดี ได้มาตรฐานตามที่กำหนด กล่าวคือผลรวมของคุณลักษณะและคุณสมบัติของผลิตภัณฑ์ข้อมูลซึ่งพึงประสงค์ทุกประการของผลการปฏิบัติงานตามดัชนีตัวชี้วัดคุณภาพและองค์ประกอบที่กำหนดไว้ ข้อมูลที่เหมาะสมกับการใช้งานตอบสนองต่อความต้องการที่กำหนด และตรงตามวัตถุประสงค์

การบริหารจัดการคุณภาพข้อมูล  
(Data Quality Management)

กระบวนการที่เกี่ยวข้องกับการวางแผน การดำเนินการ และการควบคุมกิจกรรมต่าง ๆ รวมถึงการปรับปรุง เพื่อให้ข้อมูลมีคุณภาพ มีความน่าเชื่อถือสามารถนำไปใช้ประกอบการวิเคราะห์และตัดสินใจทางธุรกิจได้อย่างถูกต้องเหมาะสม

คำอธิบายข้อมูลเชิงธุรกิจ  
(Business Metadata)

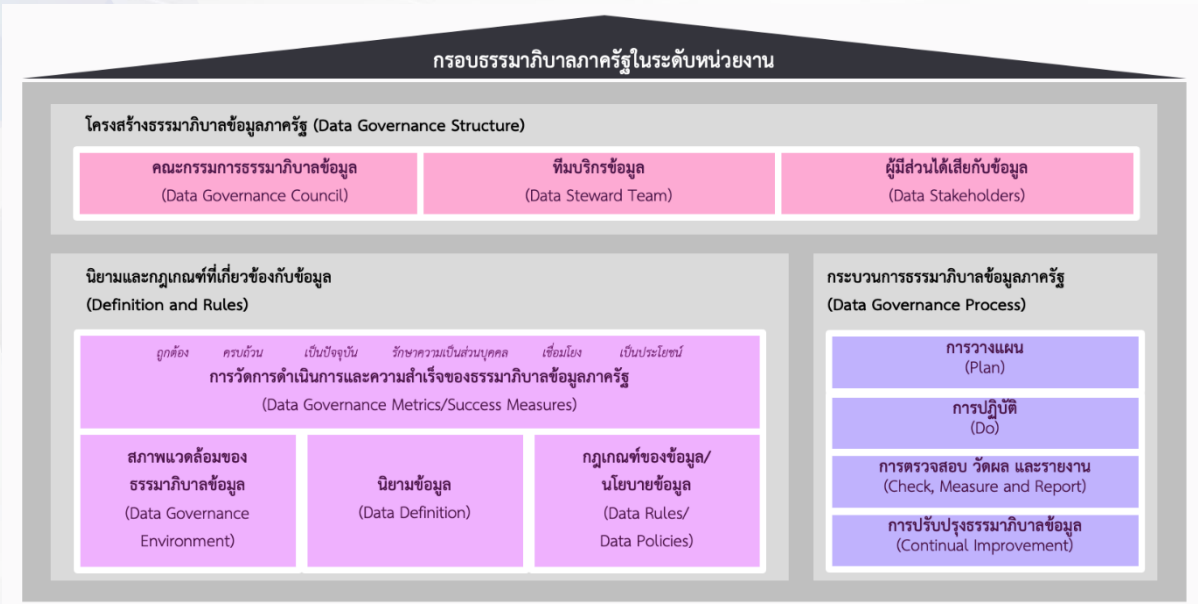
คำอธิบายชุดข้อมูลที่ให้รายละเอียดของชุดข้อมูลในด้านธุรกิจเหมาะสำหรับผู้ใช้งานข้อมูลในการประกอบการดำเนินงานธุรกิจในองค์กร เช่น ชื่อข้อมูล ชื่อเจ้าของข้อมูล คำอธิบายอย่างย่อ วันที่เริ่มต้นใช้งาน วันที่ทำการเปลี่ยนแปลงข้อมูล ภาษาที่ใช้ชื่อฟิลด์ข้อมูล (ชื่อพนักงาน นามสกุล เพศ) เป็นต้น

คำอธิบายข้อมูลเชิงเทคนิค  
(Technical Metadata)

คำอธิบายชุดข้อมูลที่ให้รายละเอียดของชุดข้อมูลในด้านเทคนิคเหมาะสำหรับผู้บริหารจัดการข้อมูลในการประกอบการดำเนินงานด้านบริหารจัดการข้อมูลเช่น ชื่อตารางข้อมูลในฐาน ข้อมูล ชื่อฟิลด์ข้อมูลในตารางข้อมูล ประเภทข้อมูล (เช่น ตัวเลข ตัวหนังสือ หรือวันที่) ความกว้างของฟิลด์ข้อมูล (เช่น 10 ตัวอักษร 50 ตัวอักษร หรือ 100 ตัวอักษร) คีย์ข้อมูล รวมไปถึงข้อมูลสำหรับการสำรองข้อมูล (Backup) และกู้คืนข้อมูล (Restore) เป็นต้น



# ภาพรวมของมาตรฐานเรื่อง การกำกับดูแลข้อมูล (Data Governance Standard) ของกรมประชาสัมพันธ์



## 1. วิสัยทัศน์ธรรมาภิบาลข้อมูลของกรมประชาสัมพันธ์

กรมประชาสัมพันธ์เป็นองค์การที่ได้รับความน่าเชื่อถือด้านข้อมูลข่าวสารเพื่อพัฒนาคุณภาพชีวิตประชาชนและสร้างภาพลักษณ์ที่ดีของประเทศ

## 2. พันธกิจธรรมาภิบาลข้อมูลของกรมประชาสัมพันธ์

เป็นองค์การหลักในการบริหารจัดการข้อมูล และข่าวสารทั้งปวง ในการสื่อสารประชาสัมพันธ์อย่างมีประสิทธิภาพ ถูกต้อง และนำไปใช้ประโยชน์ในการพัฒนาชาติ และพัฒนาสังคมได้



# 1. การกำกับดูแลข้อมูล

## 1.1 การจัดโครงสร้างองค์กรในการกำกับดูแลข้อมูล

กรมประชาสัมพันธ์ควรกำหนดโครงสร้างองค์กรและบทบาทหน้าที่ความรับผิดชอบในกระบวนการกำกับดูแลข้อมูลอย่างชัดเจนเป็นลายลักษณ์อักษรโดยครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

### หน้าที่ความรับผิดชอบของคณะกรรมการกรมประชาสัมพันธ์

คณะกรรมการกรมประชาสัมพันธ์ มีหน้าที่ในการกำกับดูแลให้กรมประชาสัมพันธ์ดำเนินการด้านที่เกี่ยวข้องกับการกำกับดูแลข้อมูลที่เหมาะสมกับขนาด ลักษณะการดำเนินธุรกิจ ความซับซ้อน และความเสี่ยงด้านข้อมูลของกรมประชาสัมพันธ์รวมทั้งสอดคล้องกับกลยุทธ์ทางธุรกิจโดยควรกำหนดหน้าที่ความรับผิดชอบในการกำกับดูแลข้อมูลอย่างชัดเจน สอดคล้องตามหลักการ

3 Line of Defense และให้ดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้

- (1) กำกับดูแลให้กรมประชาสัมพันธ์มีการกำหนดนโยบายการกำกับดูแลข้อมูล โดยได้รับการพิจารณาอนุมัติจากคณะกรรมการกรมประชาสัมพันธ์หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย และทบทวนอย่างน้อยปีละ 1 ครั้ง หรือ ทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
- (2) กำกับดูแลให้มีการนำนโยบายการกำกับดูแลข้อมูลที่ผ่านการอนุมัติจากคณะกรรมการกรมประชาสัมพันธ์หรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย มาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารจัดการข้อมูลรวมถึงดูแลใหม่ การนำไปปฏิบัติอย่างเหมาะสมและมีการทบทวนและประเมินประสิทธิภาพของนโยบายอย่างน้อยปีละ 1 ครั้ง หรือ ทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
- (3) กำกับดูแลให้มีผู้รับผิดชอบในการปฏิบัติหน้าที่ ครอบคลุมในเรื่องดังต่อไปนี้
  - การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูล
  - การบริหารความเสี่ยงด้านข้อมูล
  - การกำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับข้อมูล
  - การตรวจสอบการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล
- (4) จัดให้มีโครงสร้างและกำหนดหน้าที่ความรับผิดชอบเกี่ยวกับการบริหารจัดการข้อมูล โดยเป็นไปตามหลักการแบ่งแยกหน้าที่ความรับผิดชอบ 3 ระดับ (Three Lines of Defense) เพื่อให้มีการกำหนดหน้าที่ ความรับผิดชอบอย่างชัดเจนและมีการถ่วงดุลอำนาจในแต่ละระดับอย่างเหมาะสม



- (5) กำกับดูแลให้มีการสร้างความรู้และความตระหนักรู้ด้านการกำกับดูแลข้อมูลในองค์กรแก่ คณะกรรมการ  
กรมประชาสัมพันธ์ ผู้บริหาร และบุคลากรทุกระดับขององค์กร เพื่อสื่อสารให้เกิดความเข้าใจ ความเข้าใจ  
ถึงความสำคัญของการใช้ข้อมูลอย่างปลอดภัย
- (6) จัดสรรทรัพยากรและงบประมาณ เพื่อรองรับการดำเนินการด้านการกำกับดูแลและบริหาร จัดการข้อมูล  
แก่หน่วยงานที่เกี่ยวข้องทั้งในด้านบุคลากรและเครื่องมือให้เพียงพอที่จะสนับสนุนการปฏิบัติงาน  
ที่เกี่ยวข้องกับการกำกับดูแลข้อมูล

ทั้งนี้ คณะกรรมการกรมประชาสัมพันธ์สามารถมอบหมายให้คณะกรรมการชุดย่อยที่มีอยู่แล้ว  
ในปัจจุบันหรือ พิจารณาจัดตั้งคณะกรรมการกำกับดูแลข้อมูล (Data Governance Committee) ขึ้นมาเป็น  
การเฉพาะ เพื่อทำหน้าที่รับผิดชอบงานด้านการกำกับดูแลการบริหารจัดการข้อมูลโดยคณะกรรมการชุดย่อยหรือ  
คณะกรรมการกำกับดูแลข้อมูลควรประกอบด้วยผู้บริหารจากหน่วยงานที่มีความเข้าใจในข้อมูลที่สำคัญของ  
กรมประชาสัมพันธ์รวมทั้งผู้บริหารที่เกี่ยวข้องดังต่อไปนี้

- (1) ผู้บริหารด้านเทคโนโลยีสารสนเทศ (Chief Information Officer)
- (2) ผู้บริหารด้านบริหารจัดการข้อมูล (Chief Data Officer)
- (3) ผู้บริหารด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (Chief Information Security Officer)
- (4) ผู้บริหารระดับสูงด้านความเสี่ยง (Chief Risk Officer)
- (5) ผู้บริหารจากส่วนงานต่าง ๆ ที่เกี่ยวข้องซึ่งมีความรู้ความเข้าใจในข้อมูลที่เป็นข้อมูลสำคัญ  
ของกรมประชาสัมพันธ์

\*\*\* ตำแหน่งเปลี่ยนให้สอดคล้องกับกรมประชาสัมพันธ์



## การปฏิบัติหน้าที่ที่เกี่ยวข้องกับการบริหารจัดการข้อมูล

### การกำกับดูแลข้อมูล และการบริหารจัดการข้อมูล

กรมประชาสัมพันธ์ควรจัดให้มี คณะกรรมการชุดย่อย (Data Governance Committee) เพื่อปฏิบัติหน้าที่ในการกำกับดูแลข้อมูลและบริหารจัดการข้อมูลโดยควรดำเนินการอย่างน้อยใน เรื่องดังต่อไปนี้



- (1) กำหนดนโยบายและระเบียบวิธีปฏิบัติที่เกี่ยวกับการกำกับดูแลข้อมูลและบริหารจัดการข้อมูล รวมทั้งทบทวนหรือปรับปรุงให้เป็นปัจจุบันอยู่เสมอ โดยควรทบทวนอย่างน้อย ปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
- (2) จัดให้มีการสื่อสารให้ความรู้เกี่ยวกับนโยบาย และระเบียบวิธีปฏิบัติที่เกี่ยวกับการกำกับดูแลข้อมูล และบริหารจัดการข้อมูล ครอบคลุมทุกระดับของการบริหารจัดการข้อมูล เพื่อให้บุคลากรทุกระดับ เกิดความตระหนักในการใช้ข้อมูลและสามารถนำไปปฏิบัติได้อย่าง ถูกต้องเหมาะสม
- (3) ติดตามสถานะในเรื่องที่เกี่ยวข้องกับการกำกับดูแลข้อมูลและบริหารจัดการข้อมูล รายงานผล ประเด็นปัญหา หรือความเสี่ยงที่พบต่อคณะกรรมการกรมประชาสัมพันธ์ หรือ คณะกรรมการชุดย่อย หรือคณะกรรมการกำกับ ดูแลข้อมูล ตามระยะเวลาที่เหมาะสมเพียงพอ
- (4) กำกับดูแลให้มั่นใจว่ามีการนำนโยบาย และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแล ข้อมูล และบริหารจัดการข้อมูลไปปฏิบัติในทุกระดับขององค์กร รวมถึงกำหนดบทบาท หน้าที่ความรับผิดชอบในการอนุมัติหรือควบคุมดูแลการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การอนุมัติการเข้าถึง การใช้และการเผยแพร่ข้อมูล เป็นต้น
- (5) กำกับดูแลให้มีหน่วยงานหรือผู้รับผิดชอบบริหารจัดการคำอธิบายชุดข้อมูล (Metadata) เพื่อทำหน้าที่ในการจัดทำ ปรับปรุงแก้ไข และสอบทานคำอธิบายชุดข้อมูลให้เป็นปัจจุบัน

ทั้งนี้ เพื่อให้การดำเนินการด้านการกำกับดูแลข้อมูล และบริหารจัดการข้อมูลมีประสิทธิภาพ กรมประชาสัมพันธ์สามารถพิจารณากำหนดให้มีคณะทำงานหรือบุคลากรเพื่อดำเนินการในเรื่อง ดังต่อไปนี้

- คณะทำงานที่ปฏิบัติหน้าที่ด้านการบริการข้อมูล (Data Steward) เพื่อดำเนินการอย่างน้อย ในเรื่องดังต่อไปนี้

- (1) สนับสนุนให้เกิดการกำกับดูแลข้อมูล และบริหารจัดการข้อมูลภายในองค์กร โดย รับคำสั่งโดยตรง จากคณะกรรมการชุดย่อยที่ปฏิบัติหน้าที่ในการกำกับดูแลข้อมูลและ บริหารจัดการข้อมูล เพื่อสร้างความมั่นใจ ว่าการบริหารจัดการข้อมูลสอดคล้องกับ นโยบายและระเบียบวิธีปฏิบัติขององค์กร





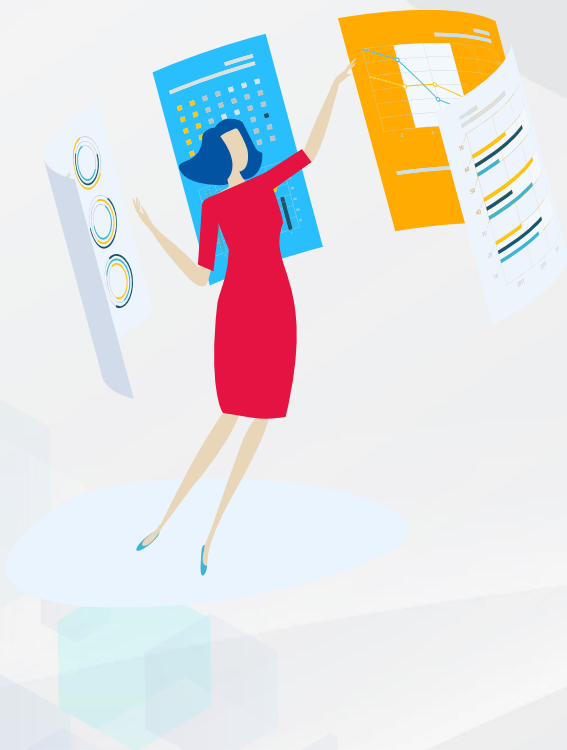
- (2) กำหนดให้มีหัวหน้าบริการข้อมูล (Lead Data Steward) โดยควรเป็นหนึ่งในคณะกรรมการชุดย่อยที่ปฏิบัติหน้าที่ในการกำกับดูแลข้อมูลและบริหารจัดการข้อมูล
- (3) กำหนดให้มีบุคลากรที่บริการข้อมูลด้านธุรกิจ (Business Data Steward) ปฏิบัติหน้าที่รับผิดชอบในการนิยามคุณลักษณะข้อมูลที่มีคุณภาพ รวมถึงนิยามของคำอธิบายชุดข้อมูล(Metadata) ที่สำคัญภายในองค์กร ทั้งนี้บริการข้อมูลด้านธุรกิจควรประกอบด้วยบุคลากรจากหลายหน่วยงานที่มีชุดข้อมูลที่สำคัญของกรมประชาสัมพันธ์ เพื่อสามารถนิยามข้อมูลที่มีคุณภาพ และคำอธิบายชุดข้อมูลได้อย่างชัดเจนที่สุด
- (4) กำหนดให้มีบุคลากรที่บริการข้อมูลด้านเทคนิค (Technical Data Steward) ปฏิบัติหน้าที่ให้การสนับสนุนด้านเทคโนโลยีสารสนเทศ รวมถึงข้อเสนอแนะเชิงเทคนิคแก่บริการข้อมูลด้านธุรกิจ เช่น การนิยามคำอธิบายชุดข้อมูลเชิงเทคนิค (Technical Metadata) ทั้งนี้ บริการข้อมูลด้านเทคนิคควรมาจากฝ่ายเทคโนโลยีสารสนเทศขององค์กร

- **กรมประชาสัมพันธ์ควรกำหนดบุคลากรหรือหน่วยงานที่เป็นเจ้าของข้อมูล (Data Owners) เพื่อดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้**

- (1) กำหนดให้มีบุคลากรหรือหน่วยงานที่เป็นเจ้าของข้อมูล ซึ่งปฏิบัติหน้าที่รับผิดชอบดูแลชุดข้อมูล โดยตรงในแต่ละชุดข้อมูลที่สำคัญ โดยทั่วไปควรเป็นผู้บริหารจากหน่วยงานที่รับผิดชอบชุดข้อมูลที่สำคัญภายในองค์กร
- (2) กำหนดให้มีบุคลากรหรือหน่วยงานที่เป็นเจ้าของข้อมูล ซึ่งปฏิบัติหน้าที่ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลที่ได้รับมอบดูแลอยู่ รวมถึงให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

- **กรมประชาสัมพันธ์ควรจัดให้มีคณะทำงานที่ปฏิบัติหน้าที่บริหารจัดการข้อมูล (Data Management Team) เพื่อดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้**

- (1) ปฏิบัติหน้าที่สนับสนุนการดำเนินการบริหารจัดการข้อมูลในด้านเทคโนโลยีสารสนเทศ เช่น การจัดทำสถาปัตยกรรมข้อมูล การจัดการฐานข้อมูล การวิเคราะห์ข้อมูล การตรวจสอบคุณภาพข้อมูล รวมถึงการดำเนินการอื่นที่สนับสนุนให้กิจกรรมที่ใช้ข้อมูลภายในองค์กรมีประสิทธิภาพมากยิ่งขึ้น



## การบริหารความเสี่ยงด้านข้อมูล

ติดตามและบริหารจัดการความเสี่ยงด้านข้อมูลตลอดวงจรชีวิตให้เหมาะสมและเป็นไปตามแนวทางการบริหารจัดการความเสี่ยงขององค์กร เพื่อหลีกเลี่ยงโอกาสเกิดความเสี่ยงที่อาจส่งผลกระทบต่อการทำงานขององค์กร โดยมีการดำเนินการดังต่อไปนี้

- จัดทำกรอบและกระบวนการบริหารความเสี่ยงขององค์กรให้ครอบคลุมความเสี่ยงด้านข้อมูล รวมทั้งสนับสนุนให้หน่วยงานต่าง ๆ ให้มีการประเมินความเสี่ยงด้านข้อมูล
- หน่วยงานกลางที่มีหน้าที่ในการกำกับดูแลและมีความเข้าใจในการบริหารจัดการข้อมูล ดำเนินการให้คำปรึกษา ติดตาม และทบทวนความเสี่ยงด้านข้อมูลให้อยู่ในระดับที่ยอมรับได้ รวมทั้งรวบรวมและเชื่อมโยงความเสี่ยงด้านข้อมูลกับความเสี่ยงด้านอื่นขององค์กรและนำเสนอผลการบริหารจัดการความเสี่ยงต่อคณะกรรมการที่เกี่ยวข้องและผู้บริหารองค์กร



## การกำกับการปฏิบัติตามกฎหมายและหลักเกณฑ์ เกี่ยวข้องกับข้อมูล

องค์กรควรรักษาความมั่นคงปลอดภัยของข้อมูลและการรักษาความเป็นส่วนตัวของข้อมูลตลอดวงจรชีวิตให้สอดคล้องกับระดับความเสี่ยงของข้อมูล ให้เป็นไปตามกฎเกณฑ์และกฎหมายที่เกี่ยวข้อง โดยดำเนินการกำกับดูแลให้เป็นไปตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องกับข้อมูลดังต่อไปนี้

- มีการรักษาความมั่นคงปลอดภัยของข้อมูลที่ครอบคลุมการรับส่งข้อมูลผ่านเครือข่าย การสื่อสาร การจัดเก็บหรือใช้ข้อมูลบนระบบงานและสื่อบันทึกข้อมูลต่าง ๆ การเก็บรักษาและการทำลายข้อมูล รวมถึงกรณีที่ต้องมีการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้สอดคล้องกับระดับความเสี่ยงของข้อมูล ทั้งนี้ องค์กรสามารถอ้างอิงแนวทางการรักษาความมั่นคงปลอดภัยร่างนโยบายที่เกี่ยวข้องต่อการบริหารจัดการธรรมาภิบาลข้อมูลว่าด้วยหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ขององค์กร รวมถึงแนวปฏิบัติอื่นที่เกี่ยวข้อง
- มีการรักษาความเป็นส่วนตัวของข้อมูล ให้สอดคล้องกับกฎเกณฑ์และกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยต้องมีการเก็บรวบรวมใช้งาน หรือเปิดเผยข้อมูลส่วนบุคคลเท่าที่จำเป็น ภายใต้วัตถุประสงค์ที่กำหนดไว้ และคำนึงถึงสิทธิของเจ้าของข้อมูล
- มีการดูแลข้อมูลของผู้ใช้บริการให้เป็นไปตามมาตรฐานขั้นตอนสำหรับการดูแลข้อมูลของผู้ใช้บริการตามที่กำหนดในคู่มือบริหารจัดการข้อมูลที่ดี (Data Governance Handbook) และเป็นไปตามการบริหารจัดการด้านการให้บริการแก่ผู้ใช้บริการอย่างเป็นธรรม (Market Conduct)

## การตรวจสอบการปฏิบัติงานที่เกี่ยวข้องกับข้อมูล

องค์กรควรเตรียมความพร้อมในการบริหารจัดการประเด็นปัญหาด้านข้อมูล เพื่อป้องกันไม่ให้เกิดเหตุการณ์ที่อำนาจไปสู่ความเสียหาย หรือเพื่อลดผลกระทบกรณีมีความเสียหายเกิดขึ้นแล้ว

- มีกระบวนการติดตามและบริหารจัดการประเด็นปัญหาด้านข้อมูล ทั้งการตรวจจับ การระบุการยับยั้งปัญหา การวิเคราะห์หาสาเหตุ การรวบรวมหลักฐานหรือเอกสาร การแก้ไขปัญหา การบริหารจัดการให้สามารถกลับมาดำเนินธุรกิจได้ตามปกติ รวมถึงการปรับปรุงกระบวนการควบคุม เพื่อลดโอกาสที่จะเกิดปัญหาที่คล้ายกันในอนาคต ในกรณีที่ประเด็นปัญหาที่เกิดขึ้นส่งผลกระทบต่อ
- ตรวจสอบการปฏิบัติงานและการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูล เพื่อสอบทานให้มั่นใจว่า เป็นไปตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล



### 1.2 นโยบายการกำกับดูแลข้อมูล

การกำหนดนโยบายข้อมูลจัดเป็นหนึ่งในองค์ประกอบตามกรอบธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้การบริหารจัดการข้อมูลของกรมประชาสัมพันธ์เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีคุณภาพ มีความมั่นคงปลอดภัย รวมทั้งการป้องกันภัยคุกคามหรือปัญหาที่อาจเกิดขึ้นจากการบริหารจัดการและการใช้ข้อมูล และสอดคล้องตามกรอบธรรมาภิบาลข้อมูลภาครัฐ จึงต้องมีการกำหนดให้มีแนวนโยบายการกำกับดูแลข้อมูล

#### โดเมนข้อมูล และโดเมนย่อยของข้อมูล

ในส่วนนี้เป็นการสรุปแนวคิดของโดเมนข้อมูลและโดเมนย่อยของข้อมูล เมื่อรวมกันแล้ว Data Domains และ Data Subdomains จะเป็นหน่วยงานกำกับดูแลข้อมูลในกรมประชาสัมพันธ์

#### ประเภทของโดเมนข้อมูล

โดเมนข้อมูล หมายถึง ชุดข้อมูลที่ครอบคลุมแขนงของข้อมูลทั้งหมด (เช่น ข้อมูลพนักงาน) มีการกำหนดขอบเขตของโดเมนข้อมูล เพื่อให้แน่ใจว่าไม่มีข้อมูลที่ไม่มีการอ้างสิทธิ์หรือทับซ้อนกันระหว่างโดเมนข้อมูลสองโดเมน โดเมนข้อมูลได้รับการจัดการโดยบริกรข้อมูล (Data Stewards) ซึ่งมีบทบาทและความรับผิดชอบอธิบายไว้ในส่วนถัดไป เมื่อข้อมูลสำหรับแขนงข้อมูลหนึ่งมีการกระจายการดำเนินงานระหว่างธุรกิจหลายแห่ง โดเมนย่อยของข้อมูลเหล่านี้จะจัดแนวเป็นโดเมนข้อมูลเดียว



กรมประชาสัมพันธ์จะมีรูปแบบการดำเนินงานแบบรวมศูนย์ ซึ่งมีความสอดคล้องระหว่างส่วนกลาง การควบคุมทั่วทั้งกลุ่ม (เช่น หัวหน้าฝ่ายจัดการข้อมูล) และหน่วยงานระดับโดเมนข้อมูลหรือโดเมนย่อยข้อมูล (เช่น บริการข้อมูล) สำหรับการกำกับดูแลข้อมูล โมเดลการดำเนินงานแบบรวมศูนย์ให้ประโยชน์ในด้านขนาดและความสม่ำเสมอจากการรวมศูนย์ ในขณะที่ช่วยให้ธุรกิจมีความยืดหยุ่นในการตอบสนองความต้องการด้านการกำกับดูแลข้อมูลเฉพาะของตน

รูปแบบการดำเนินงานแบบรวมศูนย์ต้องการบทบาททั้งในสำนักงานกลางที่สอดคล้องกับหัวหน้าฝ่ายจัดการข้อมูล และในธุรกิจ (เช่น บริการข้อมูล) เพื่อนำมาตรฐานทั่วไปไปใช้ในกรมประชาสัมพันธ์อย่างมีประสิทธิภาพ และรับประกันคุณภาพและความสอดคล้องของข้อมูล ด้วยเหตุนี้ โดเมนข้อมูลและโดเมนย่อยของข้อมูลจึงเป็นรากฐานที่สำคัญของรูปแบบการดำเนินงานแบบรวมศูนย์

กรมประชาสัมพันธ์จะมีโดเมนข้อมูล 4 ประเภท ได้แก่

- โดเมนข้อมูลธุรกรรม (Transactional Data Domains) : โดเมนข้อมูลเหล่านี้ประกอบด้วยข้อมูลที่สร้างขึ้นโดยแอปพลิเคชันที่จัดการกระบวนการทางธุรกิจ เช่นเดียวกับข้อมูลการดำเนินงานที่ข้อมูลถูกเก็บไว้ชั่วคราวหรือถาวร (เช่น ธุรกรรมบัตรเครดิต) ซึ่งข้อมูลที่ลูกค้าพบส่วนใหญ่เป็นข้อมูลธุรกรรม
- โดเมนข้อมูลอ้างอิง (Reference Data Domains) : โดเมนข้อมูลเหล่านี้ประกอบด้วยข้อมูลทั้งหมดที่ค่อนข้างคงที่เมื่อเวลาผ่านไป และจำเป็นสำหรับสายธุรกิจหลายสาย (เช่น ข้อมูลลูกค้า ข้อมูลผลิตภัณฑ์) ข้อมูลส่วนใหญ่มีการแลกเปลี่ยนกับบุคคลที่สามสอดคล้องกับข้อมูลอ้างอิง
- โดเมนข้อมูลที่ได้รับมา (Derived Data Domains) : โดเมนข้อมูลเหล่านี้ประกอบด้วยข้อมูลที่ได้รับการจัดการและรวบรวมตามธุรกรรมและข้อมูลอ้างอิงเพื่อตอบคำถามเฉพาะ โดยทั่วไปจะรวมถึงการวิเคราะห์ รายงาน ความเสี่ยง และกิจกรรมการประมวลผลข้อมูลที่คล้ายคลึงกัน
- โดเมนข้อมูลที่ค้นพบ (Discovered Data Domains) : โดเมนข้อมูลเหล่านี้ประกอบด้วยข้อมูลที่ได้รับการจัดการและรวบรวมตามธุรกรรมและข้อมูลอ้างอิงเพื่อค้นหาข้อมูลเชิงลึกที่ไม่รู้จักมาก่อน โดยทั่วไปจะรวมถึงการวิเคราะห์ การทดสอบผลิตภัณฑ์ และกิจกรรมการค้นหาข้อมูลที่คล้ายคลึงกัน

### บทบาทหน้าที่ และความรับผิดชอบ

ส่วนนี้อธิบายถึงบทบาทและความรับผิดชอบหลักในการดำเนินการตามนโยบายและมาตรฐานสนับสนุนทั่วทั้งกรมประชาสัมพันธ์ บทบาทการกำกับดูแลข้อมูลที่กำหนดซึ่งกำหนดไว้ในนโยบายนั้นมีอำนาจโดยคณะกรรมการบริหารกรมประชาสัมพันธ์ เพื่อใช้และดำเนินการตามวิจารณ์ของตนเอง เพื่อปฏิบัติตามความรับผิดชอบที่กำหนดไว้ในเอกสารนี้

### บทบาทระดับโดเมนข้อมูลและระดับโดเมนย่อยของข้อมูล

โดเมนข้อมูลและโดเมนย่อยของข้อมูลประกอบด้วยกลุ่มอิสระที่สร้างและจัดการข้อมูล และมีโอกาสแรกในการระบุความเสี่ยงระหว่างกิจกรรมทางธุรกิจในแต่ละวัน พนักงานที่ได้รับมอบหมายบทบาทเหล่านี้จะต้องมีวุฒิภาวะและความอาวุโสในการดำเนินการตามคำสั่งนโยบายและมาตรฐานสนับสนุนอย่างมีประสิทธิภาพ ควรสร้างบทบาทการกำกับดูแลข้อมูลต่อไปนี้เป็นสำหรับแต่ละโดเมนข้อมูลและโดเมนย่อยข้อมูลในกรมประชาสัมพันธ์



- เจ้าของข้อมูล (Data Owner) : กรรมการหรือผู้จัดการที่เป็นเจ้าของการกำกับดูแลข้อมูลในโดเมนข้อมูลหรือโดเมนย่อยของข้อมูล ความรับผิดชอบรวมถึง :
  - กำหนดกลยุทธ์ข้อมูล ลำดับความสำคัญ และเป้าหมายสำหรับข้อมูลภายในโดเมนข้อมูลหรือโดเมนย่อยข้อมูล
  - สนับสนุนและอนุญาตการริเริ่มข้อมูลใหม่ภายในขอบเขตของโดเมนข้อมูลหรือโดเมนย่อยข้อมูล
  - ทำงานร่วมกับหัวหน้าฝ่ายการจัดการข้อมูลในการพัฒนาความคิดริเริ่มระดับโดเมนข้อมูลหรือโดเมนย่อยของข้อมูลในระดับกลุ่มที่ต้องการการลงทุนจำนวนมาก
  - ทำหน้าที่เป็นบุคคลติดต่อในการยกระดับสำหรับปัญหาโดเมนข้อมูลหรือโดเมนย่อยข้อมูล
- บริกรข้อมูล (Data Steward) : ผู้เชี่ยวชาญเฉพาะเรื่องของข้อมูลในโดเมนข้อมูลหรือโดเมนย่อยข้อมูล ซึ่งมีหน้าที่รับผิดชอบในการรับรองว่าข้อมูลได้รับการจัดการตามนโยบายและมาตรฐานที่สนับสนุนความรับผิดชอบรวมถึง :
  - แปลกกลยุทธ์ข้อมูลสำหรับโดเมนข้อมูลหรือโดเมนย่อยข้อมูลเป็นความคิดริเริ่มที่ดำเนินการได้
  - พัฒนาแผนธุรกิจ โดยละเอียดสำหรับกรณีการใช้งานที่เสนอ
  - จัดการการควบคุมการเข้าถึง ตรวจสอบการกระจายของข้อมูล อนุมัติการจัดเตรียมข้อมูลให้กับผู้ใช้ที่ได้รับอนุญาต และสนับสนุนผู้ใช้ที่ได้รับอนุญาตในฐานะผู้เชี่ยวชาญเฉพาะเรื่องสำหรับข้อมูลในโดเมนข้อมูลหรือโดเมนย่อยข้อมูล
  - ทำงานร่วมกับสำนักงานหัวหน้าฝ่ายจัดการข้อมูลเพื่อใช้กรอบงานและจัดประเภทข้อมูลตามผลกระทบ
  - กำหนดแหล่งที่มาอย่างเป็นทางการของข้อมูล ตรวจสอบเส้นทางในการนำเข้าของข้อมูล และจัดการข้อมูลเมทาดาตา
  - กำหนดกฎทางธุรกิจที่เกี่ยวข้องกับการวัดและเมตริกคุณภาพของข้อมูล
  - อนุมัติและจัดลำดับความสำคัญของแผนการแก้ไขคุณภาพข้อมูล
- บริกรแพลตฟอร์ม (Platform Steward) : รับผิดชอบในการพัฒนาหรือจัดการระบบประมวลผลข้อมูลและโครงสร้างพื้นฐานที่สนับสนุนการกำกับดูแลข้อมูล ความรับผิดชอบรวมถึง :
  - ดำเนินการความคิดริเริ่มด้านข้อมูลใหม่และให้ข้อมูลตามเวลาและประมาณการค่าใช้จ่าย
  - กำหนดและใช้การควบคุมทางเทคนิค และพัฒนาหลักฐานการปฏิบัติตามนโยบายและมาตรฐานสนับสนุน
  - ใช้การควบคุมการเข้าถึง เพื่อให้ข้อมูลแก่พนักงานหรือระบบที่ได้รับอนุญาต การติดตามและควบคุมการเคลื่อนย้ายข้อมูล และทำให้มั่นใจว่ามีการแบ่งปันข้อมูลจากแหล่งข้อมูลที่เป็นทางการอย่างมีประสิทธิภาพ
  - รักษาแบบจำลองข้อมูลเชิงตรรกะและกำหนดข้อกำหนดทางเทคนิค
  - ตรวจสอบให้แน่ใจว่าข้อมูลได้รับการจัดเตรียมในระบบบันทึกที่เหมาะสม
  - แปลกกฎทางธุรกิจเป็นกฎคุณภาพข้อมูลและสร้างการควบคุมคุณภาพข้อมูล
  - วิเคราะห์ต้นตอของปัญหาคุณภาพของข้อมูล และออกแบบและดำเนินกิจกรรมการแก้ไขโดยร่วมมือกับหัวหน้าฝ่ายจัดการข้อมูล



## บทบาทระดับกรมประชาสัมพันธ์

หัวหน้าฝ่ายจัดการข้อมูลมีโอกาสครั้งที่สองในการระบุความเสี่ยงและรับผิดชอบในการกำกับดูแลที่เป็นอิสระ บทบาทระดับกลุ่มจากส่วนกลางประกอบด้วย :

- หัวหน้าฝ่ายจัดการข้อมูล : รับผิดชอบในการกำกับดูแลข้อมูลทั้งกรมฯ และกลยุทธ์
- หัวหน้าฝ่ายกำกับดูแลข้อมูล : สร้างและรักษานโยบายและมาตรฐานสนับสนุน จัดลำดับความสำคัญของความคิดริเริ่มด้านข้อมูลทั่วทั้งกลุ่ม และกำหนดวาระสำหรับการประชุมคณะกรรมการบริหารกรมประชาสัมพันธ์ และคณะกรรมการด้านข้อมูลที่เกี่ยวข้อง
- ผู้นำด้านคุณภาพข้อมูล : ตรวจสอบและนำมาตราฐานคุณภาพข้อมูล มาตรการ และเมตริกไปใช้ในโดเมนข้อมูลและโดเมนย่อยข้อมูล ติดตามแผนการแก้ไขคุณภาพข้อมูล
  - ผู้นำด้านเมทาเดตา : ให้การกำกับดูแลแหล่งข้อมูลที่ใช้งานและจัดการการเลือกองค์ประกอบข้อมูลทางเทคนิคเพื่อเปิดใช้งานเส้นทางในการนำเข้าข้อมูล
  - ผู้นำด้านสถาปัตยกรรมข้อมูล : กำหนดสถาปัตยกรรมข้อมูลและออกแบบความคิดริเริ่มด้านข้อมูลใหม่ร่วมกับทีมสถาปัตยกรรมด้านเทคโนโลยีสารสนเทศ และทีมกำหนดกลยุทธ์ขององค์กร



หัวหน้าฝ่ายจัดการข้อมูล โดยผ่านหัวหน้าฝ่ายกำกับดูแลข้อมูล หัวหน้าฝ่ายควบคุมคุณภาพข้อมูล และหัวหน้าฝ่ายสถาปัตยกรรมข้อมูล จะต้องจัดการการรวมข้อมูลของบุคคลที่สามเข้ากับระบบประมวลผลข้อมูลของกรมประชาสัมพันธ์ เพื่อให้เป็นไปตามนโยบายและมาตรฐานสนับสนุน

## ความรับผิดชอบของคณะกรรมการ

คณะกรรมการ 3 ระดับจะมีส่วนร่วมในการกำกับดูแลข้อมูลกรมประชาสัมพันธ์ :

- คณะกรรมการบริหารกรมประชาสัมพันธ์ : กำหนดกลยุทธ์การกำกับดูแลข้อมูลสำหรับกรมประชาสัมพันธ์ นอกจากนี้ยังอนุมัติและประสานงานกิจกรรมการกำกับดูแลข้อมูลทั่วทั้งกลุ่มและทำหน้าที่เป็นผู้ประเมินเมื่อปัญหาการยกระดับ ความรับผิดชอบรวมถึง :
  - อนุมัติกลยุทธ์ด้านข้อมูลและแผนงานของกรมประชาสัมพันธ์ เพื่อให้สอดคล้องกับกลยุทธ์ทางธุรกิจ
  - อนุมัตินโยบายและมาตรฐานสนับสนุนเพื่อให้อำนาจหัวหน้าฝ่ายจัดการข้อมูล
  - อนุมัติความคิดริเริ่มที่เกี่ยวข้องกับข้อมูลที่สำคัญ
  - ติดตามและตรวจสอบความคืบหน้ากับความคิดริเริ่มด้านการกำกับดูแลข้อมูลที่สำคัญ
  - ตรวจสอบคุณภาพข้อมูลระดับสูงและมาตรวัดและตัวบ่งชี้การกำกับดูแลข้อมูล
- คณะกรรมการควบคุมการกำกับดูแลข้อมูล : หัวหน้าฝ่ายจัดการข้อมูลเป็นประธานและตรวจสอบและอนุมัติประเด็นการกำกับดูแลข้อมูลและการแก้ปัญหาตามลำดับ ความรับผิดชอบรวมถึง :
  - ทบทวนและสรุปนโยบายและมาตรฐานสนับสนุน
  - กำหนดโดเมนข้อมูล โดเมนย่อยข้อมูล และขอบเขต
  - ทำหน้าที่เป็นผู้ตัดสินใจในการยกระดับสำหรับปัญหาที่เจ้าของข้อมูล บริการข้อมูล และบริการแพลตฟอร์มไม่ได้รับการแก้ไข
  - ตรวจสอบและอนุมัติมาตรวัดคุณภาพข้อมูล

- ตรวจสอบปัญหาคุณภาพของข้อมูล
- คณะทำงาน : ประกอบด้วยหน่วยงานกำกับดูแลตามหน้าที่ (เช่น การปกป้องข้อมูล คุณภาพของข้อมูล) โดยมีส่วนร่วมจากเจ้าของข้อมูล บริการข้อมูล และบริการแพลตฟอร์ม ประชุมกันเพื่อตอบสนองความต้องการในการดำเนินงานเฉพาะ ความรับผิดชอบรวมถึง :
  - พัฒนาแผนการแก้ไขสำหรับปัญหาการกำกับดูแลข้อมูล (เช่น คุณภาพของข้อมูล)
  - ข้อมูลเมตาของเอกสาร (เช่น การตรวจสอบย้อนกลับ)
  - พัฒนาแผนธุรกิจ สำหรับการได้มาซึ่งข้อมูลจากบุคคลที่สาม
  - ตรวจสอบและอนุมัติค่าขอแบ่งปันข้อมูลที่เป็นความลับ

## นโยบาย

### ภาพรวมของนโยบาย

นโยบายกำหนดให้ปฏิบัติตามกฎระเบียบที่เกี่ยวข้องทั้งหมด รวมทั้งคำนิยามถึงปัจจัยอื่น ๆ เช่น ภาระผูกพันตามสัญญา อาจต้องใช้ข้อกำหนดทางธุรกิจที่เข้มงวดมากขึ้น บริการข้อมูลต้องระบุระบบการประมวลผลข้อมูลและกระบวนการที่ต้องการการควบคุมที่เข้มงวดมากขึ้นและปฏิบัติตามข้อกำหนดทางกฎหมายหรือข้อบังคับของธุรกิจเฉพาะเหล่านี้ ความคาดหวังทางกฎหมายหรือข้อบังคับใด ๆ ที่กำหนดและจัดทำเป็นเอกสารโดยกฎหมาย ซึ่งแตกต่างจากนโยบายและมาตรฐานสนับสนุน

### การธรรมาภิบาลข้อมูล

ต้องกำหนดเจ้าของข้อมูล บริการข้อมูล และบริการแพลตฟอร์ม สำหรับแต่ละโดเมนข้อมูลและโดเมนย่อยของข้อมูล เจ้าของข้อมูลต้องเป็นกรรมการหรือสูงกว่า และต้องรับผิดชอบในการจัดทำโปรแกรมการกำกับดูแลข้อมูล เพื่อให้มั่นใจว่าเป็นไปตามนโยบายและมาตรฐานสนับสนุน เจ้าของข้อมูลมีความรับผิดชอบสูงสุดต่อการปฏิบัติตามโดเมนข้อมูลและโดเมนย่อยข้อมูลของตน เจ้าของข้อมูลต้อง :

- สร้างโครงสร้างโปรแกรมการกำกับดูแลข้อมูลที่ยั่งยืน และรูปแบบการดำเนินงานสำหรับโดเมนข้อมูลและโดเมนย่อยของข้อมูล
- กำหนดบริการข้อมูล ซึ่งเป็นผู้เชี่ยวชาญเฉพาะเรื่องของข้อมูลในโดเมนข้อมูลหรือโดเมนย่อยของข้อมูล รวมทั้งเป็นผู้รับผิดชอบในการรับรองว่าข้อมูลได้รับการจัดการตามนโยบายและมาตรฐานสนับสนุน
- ตรวจสอบให้แน่ใจว่าได้มอบหมาย ผู้นำด้านคุณภาพข้อมูล จากหัวหน้าฝ่ายการจัดการข้อมูล และรับผิดชอบในการวัดคุณภาพข้อมูล แก้ไขปัญหา และดำเนินกิจกรรมการดำเนินงาน เพื่อรักษาข้อมูลในโดเมนข้อมูลหรือโดเมนย่อยของข้อมูล
- ตรวจสอบให้แน่ใจว่า บริการแพลตฟอร์มได้รับมอบหมายให้เป็นผู้รับผิดชอบในการพัฒนาหรือดูแลระบบการประมวลผลข้อมูลและโครงสร้างพื้นฐาน



## 2. การบริหารจัดการข้อมูล (Data Management)

### 2.1 วงจรชีวิตของข้อมูล (Data Life Cycle)

**วงจรชีวิตของข้อมูล** หรือที่เรียกว่า “Data Life Cycle” หมายถึง ช่วงเวลาทั้งหมดที่มีข้อมูลอยู่ในระบบขององค์กร ซึ่งวงจรชีวิตนี้จะครอบคลุมทุกขั้นตอนที่ข้อมูลของคุณต้องผ่าน ตั้งแต่การสร้างข้อมูลไปจนถึงทำลายข้อมูล ในวิทยาศาสตร์ สิ่งมีชีวิตทุกชนิดจะต้องผ่านช่วงต่าง ๆ ได้แก่ วัยทารก ช่วงเวลาของการเติบโต และการพัฒนาวัยเจริญพันธุ์ที่มีประสิทธิผล และวัยชรา ซึ่งขั้นตอนเหล่านี้แตกต่างกันไป เช่น ปลาแซลมอนจะตายทันทีหลังจากวางไข่ ในขณะที่มนุษย์มีชีวิตอยู่จนเป็นปู่ตายาย แม้ว่าสิ่งมีชีวิตจะอาศัยอยู่ในสภาพแวดล้อมเดียวกัน แต่ต่างก็มีวงจรชีวิตที่ไม่เหมือนกัน

ในทำนองเดียวกัน ข้อมูล หรือ Data ก็ผ่านช่วงเวลาต่าง ๆ ของชีวิตตามจังหวะของมันเอง ซึ่งโดยทั่วไปแล้ววงจรชีวิตข้อมูล หรือ Data Life Cycle จะแบ่งออกได้เป็น 6 ขั้นตอนดังนี้

#### สร้างข้อมูล (Create)

ในการเริ่มต้นของวงจรชีวิตข้อมูล หรือ Data Life Cycle ขั้นตอนลำดับแรกต้องเป็นการสร้างข้อมูล ถ้าไม่มีขั้นตอนนี้ก็จะไม่มีขั้นตอนอื่น ๆ ตามมา ทุกวันนี้ทั่วทั้งโลกมีการสร้างข้อมูลกว่า 2.5 Quintillion Bytes หรือ 2,500 ล้าน GB ต่อวัน หรือถ้าจะอธิบายให้เห็นภาพคือ “เราแต่ละคนผลิตข้อมูลกันเฉลี่ยวินาทีละ 1.7 MB” เลยทีเดียว และมีการประมาณการอีกด้วยว่า ในปี 2025 เราอาจผลิตข้อมูลเพิ่มขึ้นเป็นคนละ 463 Exabytes ต่อวัน โดยข้อมูลเหล่านี้ส่วนใหญ่ก็มาจากการใช้งานอินเทอร์เน็ตและอุปกรณ์ต่าง ๆ ของเรา, ข้อมูล Big Data จากหลายๆองค์กร, อุปกรณ์ IoT และข้อมูล Transaction ต่าง ๆ ในสกุลเงินดิจิทัลที่มีแนวโน้มเพิ่มขึ้นเรื่อย ๆ อย่างไม่มีที่สิ้นสุด



#### จัดเก็บข้อมูล (Store)

หลังจากที่มีการสร้างข้อมูลแล้ว ขั้นตอนถัดไปของวงจรชีวิตข้อมูล หรือ Data Life Cycle คือการจัดเก็บข้อมูล (Store) เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหาย หรือถูกทำลาย และให้ผู้ใช้สามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว

ซึ่งเราสามารถจัดเก็บข้อมูลได้โดยสร้างฐานข้อมูล (Databases) หรือชุดข้อมูล (Datasets) จากนั้นชุดข้อมูลเหล่านี้ อาจจะถูกจัดเก็บไว้ในระบบคลาวด์บนเซิร์ฟเวอร์ หรือใช้อุปกรณ์จัดเก็บข้อมูลทางกายภาพรูปแบบอื่น เช่น ฮาร์ดไดรฟ์ โดยวิธีการจัดเก็บข้อมูลที่ดีที่สุดจะพิจารณาตามการใช้งานและบริบทของแต่ละองค์กร



## ใช้ข้อมูล (Use)

การใช้ข้อมูล (Use) ในวงจรชีวิตข้อมูล หรือ Data Life Cycle เป็นการนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์และสนับสนุนกิจกรรมขององค์กร รวมถึงการสำรอง (Backup) ข้อมูล โดยการคัดลอกข้อมูลที่ใช้งานอยู่ในปัจจุบัน เพื่อทำสำเนา เช่น ใช้โปรแกรมในการสำรองข้อมูล เป็นการหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย ซึ่งสามารถนำข้อมูลที่สำรองไว้ในสื่อบันทึกข้อมูลกลับมาใช้งานได้ทันที โดยการกู้คืน (Restore)

## เผยแพร่ข้อมูล (Publish)

ขั้นตอนเผยแพร่ข้อมูลในวงจรชีวิตข้อมูล หรือ Data Life Cycle นี้ จะเป็นการแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition) เพื่อที่ข้อมูลเหล่านั้นจะถูกเปลี่ยนไปเป็นกิจกรรมและการตัดสินใจขององค์กร ซึ่งจะเป็นการเพิ่มคุณค่าสูงสุดให้กับข้อมูลนั้น ๆ

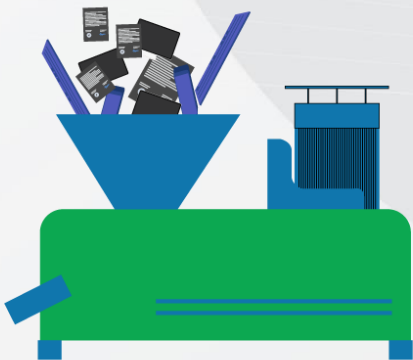
## จัดเก็บข้อมูลถาวร (Archive)

หลังจากที่ข้อมูลได้ถูกใช้ และเผยแพร่แล้ว ข้อมูลนั้น ๆ จะเข้าสู่ขั้นตอน **จัดเก็บข้อมูลถาวร** ในวงจรชีวิตข้อมูล หรือ Data Life Cycle ซึ่งจะเป็นการคัดลอกเอาข้อมูลที่มีช่วงอายุเกินช่วงใช้งาน หรือไม่ได้ใช้งานแล้ว มาทำสำเนาสำหรับการเก็บรักษา โดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

## ทำลายข้อมูล (Destroy)

เมื่อข้อมูลในกระบวนการจัดเก็บข้อมูลถาวรมีปริมาณเพิ่มขึ้นมากจนไม่สามารถจัดเก็บไว้ได้ เนื่องจากปัญหาด้านต้นทุนในการจัดเก็บข้อมูล หรือจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด ข้อมูลเหล่านั้นจะเข้าสู่ขั้นตอน **ทำลายข้อมูล** ในวงจรชีวิตข้อมูล หรือ Data Life Cycle

ความท้าทายของวงจรชีวิตข้อมูลระยะนี้ก็คือ การทำให้แน่ใจว่า ข้อมูลถูกทำลายอย่างเหมาะสม สิ่งสำคัญคือต้องตรวจสอบให้แน่ใจ ก่อนที่จะทำลายข้อมูลว่า รายการข้อมูลนั้นเกินระยะเวลาการเก็บรักษา ตามข้อบังคับที่กำหนดหรือไม่



## 2.2 การบริหารจัดการคำอธิบายชุดข้อมูล (Metadata Management)

เมทาดาตา คือข้อมูลที่อธิบายชุดข้อมูลและรวมถึงลักษณะต่าง ๆ เช่น คำจำกัดความ เจ้าของ แหล่งข้อมูลที่เป็นทางการ รูปแบบของข้อมูล มาตรฐานและเมตริกคุณภาพของข้อมูล ข้อมูลเมทาดาตาเป็นสิ่งสำคัญสำหรับผู้ใช้งานในการทำความเข้าใจข้อมูลและรายงานที่พวกเขาใช้ ขจัดความกำกวม และทำให้สามารถระบยอดผลการรายงานได้นอกจากนี้ยังเป็นสิ่งสำคัญสำหรับวิศวกรที่สนับสนุนระบบการประมวลผลข้อมูลและโครงสร้างพื้นฐานการจัดการข้อมูลเมทาดาตาเป็นวิธีปฏิบัติในการรวบรวมและกำหนดมาตรฐานข้อมูลในพจนานุกรมข้อมูลกลุ่ม ผู้นำด้านเมทาดาตาซึ่งเป็นตัวแทนของหัวหน้าฝ่ายจัดการข้อมูล จะต้อง :

- กำหนดมาตรฐานสำหรับข้อมูลเมตามตามแนวทางปฏิบัติที่ดีที่สุดระหว่างประเทศ และรับรองว่าสอดคล้องกับมาตรฐานเหล่านี้
- คิดค้นและแก้ไขอนุกรมวิธานข้อมูล รวมถึงการระบุและจัดการรายการมาตรฐานของโดเมนข้อมูลและโดเมนย่อย
- ตรวจสอบให้แน่ใจว่าไม่มีการซ้ำซ้อนสำหรับอนุกรมวิธานข้อมูลกลุ่ม
- สร้างเทมเพลตสำหรับทั้งกลุ่มสำหรับบันทึกทั้งข้อมูลเมตาของธุรกิจ (เช่น คำจำกัดความของธุรกิจ กฎด้านคุณภาพข้อมูล) และข้อมูลเมตาทางเทคนิค (เช่น รูปแบบข้อมูล) บริการข้อมูล ร่วมกับบริการแพลตฟอร์ม จะต้อง :
- ดูแลรักษาพจนานุกรมข้อมูลและรูปแบบข้อมูลสำหรับโดเมนข้อมูลและโดเมนย่อยข้อมูลที่กำหนด
- ส่งเสริมการใช้พจนานุกรมข้อมูลสำหรับโดเมนข้อมูลและโดเมนย่อยข้อมูลที่กำหนด
- รายงานการสร้างคำจำกัดความใหม่หรือการเปลี่ยนแปลงใด ๆ จากพจนานุกรมข้อมูลที่มีอยู่ไปยังเจ้าของข้อมูล



## 2.3 การบริหารจัดการคุณภาพข้อมูล (Data Quality Management)

เพื่อให้การควบคุมคุณภาพข้อมูล สำหรับการนำไปใช้ประโยชน์ในการบริหารงานและการให้บริการประชาชนของกรมประชาสัมพันธ์ โดยให้เป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานตามที่กฎหมายกำหนด โดยข้อมูลที่ได้รับการจัดเก็บนั้น กรมประชาสัมพันธ์จะคำนึงถึงคุณภาพข้อมูล (Data Quality) ในทุกชุดข้อมูล (Dataset) โดยมีการกำหนดมาตรฐาน ดังนี้

2.3.1 กำหนดมาตรฐานข้อมูลให้เป็นแบบเดียวกัน และมีการควบคุมคุณภาพข้อมูลตลอดทั้งวงจรชีวิตข้อมูล (Data Life Cycle) ของข้อมูลที่ตนเองมีหน้าที่รับผิดชอบเท่านั้น

2.3.2 กำหนดให้มีข้อกำหนดพื้นฐานของการบริหารจัดการคุณภาพข้อมูล (Data Quality Management) รวมถึงแนวทางการควบคุมและการปรับปรุงอย่างต่อเนื่อง

2.3.3 ทุกข้อมูลทุกชุดต้องมีการวัดคุณภาพข้อมูล (Data Quality) ดังนี้

- ความถูกต้อง (Accuracy)  
ข้อมูลจะมีความถูกต้องและเชื่อถือได้ขึ้นกับวิธีการที่ใช้ในการควบคุมข้อมูลนำเข้า และการควบคุมการประมวลผล การควบคุมข้อมูลนำเข้าเป็นการกระทำเพื่อให้เกิดความมั่นใจว่าข้อมูลนำเข้ามีความถูกต้องเชื่อถือได้ เพราะถ้าข้อมูลนำเข้าไม่มีความถูกต้องแล้ว ถึงแม้จะใช้วิธีการวิเคราะห์และประมวลผลข้อมูลที่ดีเพียงใด ผลลัพธ์ที่ได้ก็จะเป็นความถูกต้องหรือนำไปใช้ไม่ได้ข้อมูลนำเข้าจะต้องเป็น



ข้อมูลที่ผ่านมาตรวจสอบว่าถูกต้องแล้ว ข้อมูลบางประเภทอาจต้องแปลงให้อยู่ในรูปแบบที่เครื่องคอมพิวเตอร์สามารถเข้าใจได้อย่างถูกต้อง ซึ่งอาจต้องพิมพ์ข้อมูลมาตรวจสอบก่อนการประมวลผลถึงแม้ว่าจะมีการตรวจสอบข้อมูลนำเข้าแล้วก็ตาม ก็อาจทำให้ได้ข้อมูลที่ผิดพลาดได้ เช่น การเขียนโปรแกรมหรือใช้สูตรคำนวณผิดพลาด ดังนั้น จึงควรกำหนดวิธีการควบคุมการประมวลผล ได้แก่ การตรวจสอบยอดรวมที่ได้จากการประมวลผลแต่ละครั้งหรือการตรวจสอบผลลัพธ์ที่ได้จากการประมวลผลด้วยเครื่องคอมพิวเตอร์กับข้อมูลสมมติที่มีการคำนวณด้วยว่ามีความถูกต้องตรงกันหรือไม่

- ความครบถ้วน (Completeness)

ข้อมูลบางประเภทหากไม่ครบถ้วน จัดเป็นข้อมูลที่ด้อยคุณภาพได้เช่นกัน เช่น ข้อมูลประวัติคนไข้ หากไม่มีหมู่เลือดของคนไข้ จะไม่สามารถใช้ได้ ในกรณีที่ผู้ร้องขอข้อมูลต้องการข้อมูลหมู่เลือดของคนไข้ หรือข้อมูลที่อยู่ของลูกค้าที่กรอกผ่านแบบฟอร์ม ถ้ามีชื่อและนามสกุลโดยไม่มีข้อมูลบ้านเลขที่ ถนน แขวง/ตำบล เขต/อำเภอ หรือ จังหวัด ข้อมูลเหล่านั้นก็ไม่สามารถนำมาใช้ได้เช่นกัน

- ตรงตามความต้องการของผู้ใช้ (Relevancy)

ระดับของข้อมูลที่บริหารจัดการต้องการนำเสนอโดยตรงและมีประสิทธิภาพ โดยสามารถใช้งานได้ตามวัตถุประสงค์ ตัวอย่างเช่น ข้อมูลทางสถิติที่จะเป็นการนำเสนอในรูปแบบตารางเข้าใจง่ายและข้อความอยู่ในหลาย ๆ ย่อหน้า ซึ่งสามารถใช้งานได้ตามความต้องการ

- ความน่าเชื่อถือ (Data Integrity)

การรักษาความถูกต้องของข้อมูล ความสามารถที่จะตรวจสอบได้ว่าข้อมูลที่ได้รับมีความถูกต้อง ครบถ้วนสมบูรณ์ และไม่ถูกเปลี่ยนแปลงแก้ไขใด ๆ ไปจากเดิม โดยผู้ที่ไม่ได้รับอนุญาต หากมีการเปลี่ยนแปลงโดยผู้ได้รับอนุญาต จะต้องมีการบันทึกทุกการเปลี่ยนแปลง เพื่อการตรวจสอบกลับ การเปลี่ยนแปลงนั้น

- ความพร้อมใช้งาน (Availability)

ข้อมูลควรเข้าถึงได้ง่าย สามารถใช้งานได้จริง และสามารถใช้งานได้ตลอดเวลา ตัวอย่างเช่น นักวิเคราะห์แผนงานต้องการข้อมูลบัญชีของการประกันภัยต่อเขตต่าง ๆ แต่ข้อมูลไม่พร้อมใช้งาน จนกระทั่งต้องใช้คนเขียนโปรแกรมเพื่อดึงข้อมูลนั้นออกมา ในกรณีนี้หากข้อมูลมีความพร้อมกับความ ต้องการใช้ ผู้ใช้สามารถใช้ข้อมูลดังกล่าวได้ทันที

โดยทุกเกณฑ์ เป็นเกณฑ์เชิงปริมาณ (Quantitative Measurement)

2.3.4 การกำหนดตัวชี้วัดคุณภาพข้อมูล เช่น ความถูกต้อง ความครบถ้วน ความตรงกัน ความเป็นปัจจุบัน ความต้องการของผู้ใช้ และพร้อมใช้งาน

2.3.5 รายงานคุณภาพข้อมูล ประกอบด้วย การกำหนดระดับมิติตัวชี้วัดและค่าเป้าหมายในการประเมินคุณภาพข้อมูล จะต้องแนบไปกับการใช้ชุดข้อมูล (Dataset) และชุดคำอธิบายข้อมูล หรือเมทาดาดา

2.3.6 การฝึกอบรมเพื่อสร้างความตระหนักถึงคุณภาพของข้อมูล

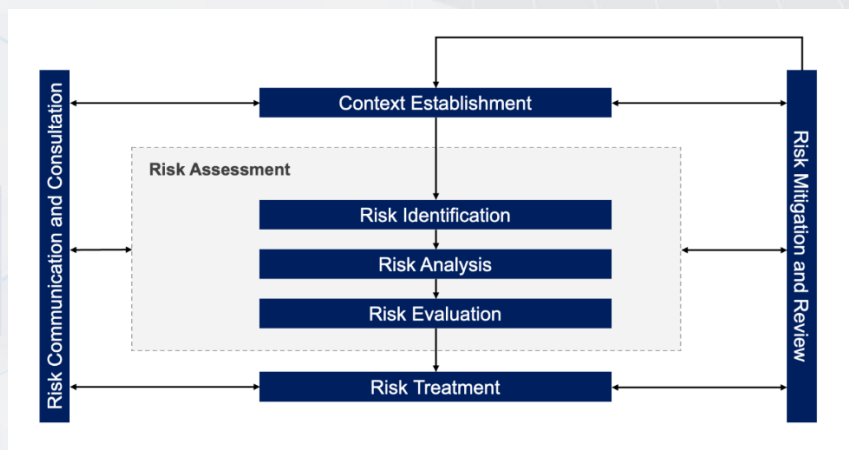






- ความเสี่ยงด้านการบริหารโครงการเทคโนโลยีสารสนเทศ (IT Project Management Risks) คือความเสี่ยงจากการบริหารโครงการเทคโนโลยีสารสนเทศ ล่าช้า หรือไม่สำเร็จ อันเนื่องมาจากการกำกับดูแลการบริหารจัดการโครงการ การมอบหมายและกำหนดขอบเขต การจัดสรรทรัพยากร เวลา เงินทุน การประสานงาน เป็นต้น
- ความเสี่ยงด้านบุคลากร (Personal Risks) คือความเสี่ยงที่เกิดจากบุคลากรขาดความรู้ ทักษะที่เพียงพอต่อการดำเนินงาน การจัดสรรบุคลากรที่ไม่เหมาะสมกับลักษณะงานที่มอบหมาย ความเสี่ยงที่เกิดจากการทุจริตของบุคลากร เป็นต้น
- ความเสี่ยงด้านการกู้ระบบจากเหตุการณ์ฉุกเฉิน และการบริหารความต่อเนื่องของการให้บริการงานเทคโนโลยีสารสนเทศ (Disaster Recovery and IT Continuity Risks) คือความเสี่ยงที่เกิดขึ้นจากภัยพิบัติ หรือเหตุการณ์ฉุกเฉินต่าง ๆ ซึ่งอาจส่งผลให้ธุรกิจเกิดความเสียหาย หยุดชะงัก หรือไม่สามารถให้บริการแก่ลูกค้าตามระยะเวลาที่กำหนดได้ เป็นต้น
- ความเสี่ยงด้านการปฏิบัติตามกฎ ระเบียบ ข้อบังคับ และกฎหมายด้านเทคโนโลยีสารสนเทศ (IT Compliance Risks) คือความเสี่ยงที่เกิดขึ้นที่ก่เกิดขึ้นจากการไม่ปฏิบัติตามกฎ ระเบียบ ข้อบังคับและกฎหมาย ซึ่งอาจส่งผลในด้านลบต่อบริบทองค์กร เช่น สูญเสียภาพลักษณ์ ถูกปรับหรือฟ้องร้อง เป็นต้น
- ความเสี่ยงด้านความปลอดภัยเทคโนโลยีสารสนเทศ (IT Security/Cyber Security Risks) คือความเสี่ยงที่เกิดขึ้นจากความไม่ปลอดภัยของเทคโนโลยีสารสนเทศ ระบบความปลอดภัยด้านโครงสร้างพื้นฐานสารสนเทศ และการใช้งานด้านไซเบอร์ สอดคล้องกับความเสี่ยงที่อาจเกิดขึ้นภายใต้หลักการสำคัญด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ 3 ประการคือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของระบบเทคโนโลยีสารสนเทศ เช่น การถูกโจมตีระบบเทคโนโลยีสารสนเทศ และ/หรือ โครงสร้างพื้นฐานสารสนเทศโดยผู้ไม่ประสงค์ดีผ่านทางระบบเครือข่าย การแพร่กระจายไวรัส ขาดการควบคุมการเข้าถึงทางกายภาพ การปลอมแปลง การแชร์ใช้งานรหัสผ่าน เป็นต้น

โดยการประเมินความเสี่ยงดังกล่าว สามารถอ้างอิงได้จากมาตรฐานสากล ISO 31000 Risk Management



รูปที่ 1 มาตรฐานสากล ISO 31000 Risk Management

## 2.5 การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

การรักษาความมั่นคงปลอดภัยของข้อมูล เป็นส่วนหนึ่งของความพยายามในวงกว้างเพื่อลดความเสี่ยงด้านความปลอดภัยในโลกไซเบอร์ โดยเฉพาะอย่างยิ่ง การคุ้มครองข้อมูลมุ่งเน้นไปที่ความเสี่ยงที่เกี่ยวข้องกับความเป็นส่วนตัวที่เกี่ยวข้องกับการละเมิดความลับ ความสมบูรณ์ หรือความพร้อมใช้งานของข้อมูลส่วนบุคคล ข้อกำหนดและการควบคุมการปกป้องข้อมูลควรได้รับการบังคับใช้และตรวจสอบเป็นระยะ โดยการกระทำข้างต้นดังกล่าวเป็นส่วนหนึ่งของความพยายามในการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่กว้างขึ้น :

- หัวหน้าฝ่ายกำกับดูแลความปลอดภัยจะต้องสร้างและบังคับใช้กระบวนการเพื่อประเมินและตัดสินใจการปฏิบัติตามมาตรฐานอย่างน้อยปีละ 2 ครั้ง
- หัวหน้าฝ่ายกำกับดูแลความปลอดภัยจะต้องประสานงานกับบริการข้อมูลและบริการแพลตฟอร์ม เพื่อออกแบบและนำแผนการแก้ไขไปปฏิบัติ เมื่อมีการระบุช่องว่างการควบคุมเทียบกับมาตรฐานในระบบการประมวลผลข้อมูล



### การจัดระดับชั้นความลับของข้อมูล

การจัดระดับชั้นความลับของข้อมูลช่วยให้กรมประชาสัมพันธ์ สามารถจัดหมวดหมู่ข้อมูลออกเป็นระดับต่าง ๆ ตามผลกระทบของข้อมูลที่ถูกรุก ข้อมูลอาจถูกคุกคามในแง่ของการรักษาความลับ ความสมบูรณ์ หรือความพร้อมใช้งาน ไม่ว่าจะโดยตั้งใจหรือโดยบังเอิญ การจัดระดับชั้นความลับของข้อมูลเป็นพื้นฐานสำหรับกรมประชาสัมพันธ์ในการตัดสินใจว่าข้อมูลต่าง ๆ ควรได้รับการคุ้มครองอย่างไร เมื่อมีการรวบรวมประมวลผลหรือเปิดเผย :



- บริการข้อมูลต้องประสานงานกับหัวหน้าฝ่ายกำกับดูแลข้อมูล และหัวหน้าฝ่ายกำกับดูแลความปลอดภัย เพื่อประเมินผลกระทบของความเสียหายต่อข้อมูลสำหรับแต่ละโดเมนย่อยของข้อมูลที่ดำเนินการจัดการ
- บริการข้อมูลต้องใช้กรอบผลกระทบของข้อมูลเพื่อประเมินผลกระทบของการประนีประนอมของโดเมนย่อยข้อมูลแต่ละรายการ
- บริการข้อมูลต้องประสานงานกับหัวหน้าฝ่ายกำกับดูแลข้อมูล และหัวหน้าฝ่ายกำกับดูแลความปลอดภัย เพื่อกำหนดระดับการจัดประเภทให้กับแต่ละโดเมนย่อยของข้อมูล
- บริการข้อมูลต้องใช้กรอบการจัดประเภทข้อมูล เพื่อจำแนกแต่ละโดเมนย่อยของข้อมูล

### การติดฉลากข้อมูล

กรมประชาสัมพันธ์ต้องติดฉลากข้อมูลตามระดับชั้นความลับเพื่อใช้ประโยชน์จากข้อมูล กิจกรรมการติดฉลากข้อมูลนี้ดำเนินการโดยใช้แอตทริบิวต์ของเมทาดาตาสำหรับข้อมูลที่จัดเก็บอย่างมีเหตุผล และใช้ป้ายกำกับทางกายภาพสำหรับข้อมูลที่จัดเก็บทางกายภาพ :

- หัวหน้าฝ่ายกำกับดูแลข้อมูลจะต้องจัดหาฉลากที่จับต้องได้ ซึ่งแสดงถึงข้อมูลที่เป็นความลับและทำให้พร้อมใช้งานสำหรับธุรกิจ (เอกสารที่ไม่มีป้ายกำกับถือเป็นเอกสารที่ใช้ภายใน)

- บริการข้อมูลต้องสร้างและบังคับใช้กระบวนการเพื่อติดตามข้อมูลทางกายภาพ (เช่น งานพิมพ์) โดยใช้ฉลากเมื่อข้อมูลดังกล่าวถูกถ่ายโอนภายในกรมประชาสัมพันธ์หรือจาก กรมประชาสัมพันธ์ไปยังบุคคลที่สาม
- บริการแพลตฟอร์มต้องสร้างและบังคับใช้การควบคุมทางเทคนิคเพื่อบันทึกการจัดประเภทของข้อมูลดิจิทัล โดยใช้แอตทริบิวต์เมทาเดตาทางเทคนิค การรักษาความลับ เมื่อข้อมูลดังกล่าวถูกสร้างขึ้นหรือถ่ายโอนไปยังกรมประชาสัมพันธ์

### การเข้ารหัสข้อมูล

การเข้ารหัสข้อมูลใช้กับทั้งการขนส่งข้อมูลและการจัดเก็บข้อมูล เป็นวิธีการหนึ่งในการรับรองว่าข้อมูลได้รับการปกป้องจากการละเมิดความลับหรือความสมบูรณ์ กรมประชาสัมพันธ์ควรใช้แนวทางปฏิบัติที่ดีที่สุดระดับสากลสำหรับการเข้ารหัสข้อมูล :

- ทีมกำกับดูแลข้อมูลต้องประสานงานกับทีมรักษาความมั่นคงความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจว่าอัลกอริทึมการเข้ารหัสที่ได้รับการพิสูจน์แล้วและความยาวของคีย์ที่เลือกเท่านั้นที่ใช้สำหรับการเข้ารหัส

## 2.6 การรักษาความเป็นส่วนตัวของข้อมูล (Data Privacy)

เพื่อลดความเสี่ยงในการแบ่งปันข้อมูลและรองรับการปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย (PDPA) กรมประชาสัมพันธ์ต้องมีการพัฒนานโยบายความยินยอมของลูกค้าแบบรวมและข้อตกลงมาตรฐานในการแบ่งปันข้อมูล เอกสารเหล่านี้จะเป็นรากฐานทางกฎหมายร่วมกันสำหรับกรมประชาสัมพันธ์ ในการรวบรวม ประมวลผล และเปิดเผยข้อมูลส่วนบุคคลระหว่างกัน และเพื่อเจรจาแบ่งปันข้อมูลกับบุคคลที่สามโดยใช้ข้อกำหนดและเงื่อนไขมาตรฐาน นอกเหนือจากนโยบายความยินยอมของลูกค้าแบบรวมและข้อตกลงมาตรฐานการแบ่งปันข้อมูลแล้ว ยังมีข้อกำหนดในการจัดเก็บและขนส่งข้อมูลที่เฉพาะเจาะจงอีกด้วย เพื่อให้มั่นใจว่ากรมประชาสัมพันธ์ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และปกป้องข้อมูลส่วนบุคคลจากการเปิดเผยโดยไม่ตั้งใจ



- บริการข้อมูลต้องสร้างและบังคับใช้กระบวนการเพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลตามที่กำหนดไว้ในกรอบข้อมูลส่วนบุคคลจะถูกแบ่งปันระหว่างกรมประชาสัมพันธ์และบุคคลอื่น ๆ ในลักษณะที่มีการเข้ารหัส หรือรักษาความมั่นคงปลอดภัย (เช่น การแฮช เป็นต้น)
- บริการแพลตฟอร์มต้องสร้างและบังคับใช้การควบคุมทางเทคนิคเพื่อให้แน่ใจว่าข้อมูลส่วนบุคคลตามที่กำหนดไว้ในกรอบข้อมูลส่วนบุคคลจะถูกแบ่งปันระหว่างกรมประชาสัมพันธ์และบุคคลอื่น ๆ ในลักษณะที่มีการเข้ารหัส หรือรักษาความมั่นคงปลอดภัย (เช่น การแฮช เป็นต้น)
- ผู้นำด้านสถาปัตยกรรมคอมพิวเตอร์จะต้องประสานงานกับทีมรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้แน่ใจว่ามีการป้องกันข้อมูลเมื่อมีการขนส่งโดยใช้การควบคุม เช่น การเข้ารหัส

### 3. แนวทางการประเมินระดับการกำกับดูแลข้อมูล (Data Governance Maturity Assessment)

#### 3.1 แนวทางการประเมินระดับการกำกับดูแลข้อมูล (Data Governance Maturity Assessment)

การประเมินความพร้อมของการกำกับดูแลข้อมูลจะทำให้องค์กรได้ทราบถึงสิ่งที่ได้ดำเนินการแล้ว และสิ่งใดบ้างที่ควรดำเนินการต่อไป เพื่อปรับปรุงการดำเนินงานให้เกิดประสิทธิภาพสูงสุด ระดับความพร้อมของการกำกับดูแลข้อมูลถูกใช้เป็นเครื่องมือในการประเมินความพร้อมของการกำกับดูแลข้อมูลโดยกรอบการกำกับดูแลข้อมูล เวอร์ชัน 1.0 ที่จัดทำโดยสำนักงานพัฒนารัฐบาลดิจิทัล (2561) ได้เสนอระดับความพร้อมและวุฒิภาวะ 5 ระดับ ดังภาพต่อไปนี้



รูปที่ 2 แนวทางการประเมินระดับการกำกับดูแลข้อมูล (Data Governance Maturity Assessment)

**Level 1 - Initial** หมายถึง ไม่มีการกำหนดมาตรฐานของกระบวนการ นั่นคือ กระบวนการถูกกำหนดขึ้นมาเฉพาะกิจ (Ad hoc) ทำให้แต่ละโครงการหรือบริการมีรูปแบบของกระบวนการที่แตกต่างกัน และอำนาจในการจัดการและกำกับดูแลข้อมูลส่วนใหญ่ถูกดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศ ทำให้การทำงานร่วมกันระหว่างฝ่ายธุรกิจและฝ่ายเทคโนโลยีสารสนเทศไม่สอดคล้องกัน

**Level 2 - Managed** หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงานหรือบริการ และมีการกำหนดบุคคลที่เกี่ยวข้องกับการกำกับติดตาม เช่น บริกรข้อมูล (Data Steward) และเจ้าของข้อมูล (Data Owner)





**Level 3 - Defined** หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงานมีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลหรือความมั่นคงปลอดภัย

**Level 4 - Quantitatively Managed** หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลและความมั่นคงปลอดภัย

**Level 5 - Optimized** หมายถึง มีการดำเนินการสอดคล้องกับระดับ 4 วิเคราะห์สาเหตุของปัญหา (Root Cause) ประกอบไปด้วย ความไม่สอดคล้องในการปฏิบัติงานกับนโยบายข้อมูล (Non-Conformation) คุณภาพข้อมูลที่ต่ำและความไม่คุ้มค่าในการบริหารจัดการข้อมูล ดำเนินการปรับปรุงกระบวนการ กฎเกณฑ์และนโยบายข้อมูล หรือโครงสร้างการกำกับดูแลข้อมูลเพื่อแก้ไขปัญหาที่พบจากผลการวิเคราะห์ และให้สอดคล้องกับความต้องการของผู้ที่เกี่ยวข้องและวัตถุประสงค์ที่เปลี่ยนไปของหน่วยงาน

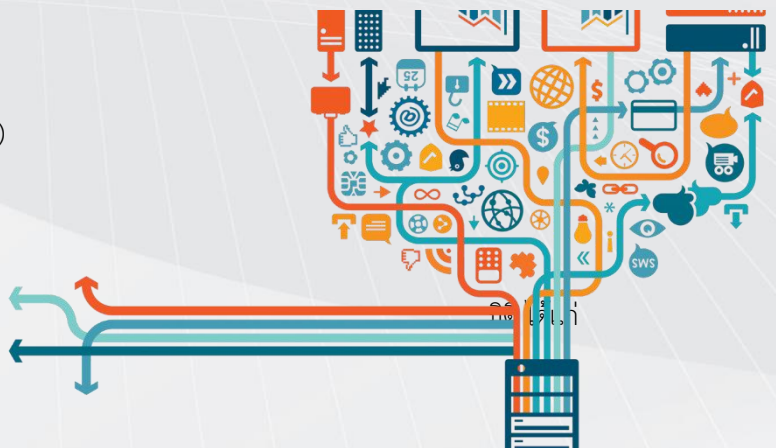
### 3.2 องค์ประกอบและมิติของการประเมินระดับความพร้อมของการกำกับดูแลข้อมูล

ตัวชี้วัดที่ระบุในกรอบการกำกับดูแลข้อมูล เป็นเพียงเกณฑ์กว้าง ๆ ที่ยังไม่สามารถสืบเสาะไปจนถึงความพร้อมในองค์ประกอบย่อย ๆ ของการกำกับดูแลข้อมูล คณะที่ปรึกษาจึงเสนอแบบประเมินความพร้อมของการกำกับดูแลข้อมูลที่พัฒนาโดย Stanford University (2011) โดยองค์ประกอบด้านการเชื่อมโยงข้อมูล ดังนั้นองค์ประกอบของการประเมินสถานะมี 6 องค์ประกอบ ได้แก่

- 1) ความตระหนักรู้ (Awareness)
- 2) การจัดระเบียบ (Formalization)
- 3) เมทาดาตา (Metadata)
- 4) การให้บริการข้อมูล (Stewardship)
- 5) คุณภาพข้อมูล (Data Quality)
- 6) ข้อมูลหลัก (Master Data)

โดยทั้ง 6 องค์ประกอบจะทำการวัดใน 3

- 1) บุคลากร (People)
- 2) นโยบาย (Policies)
- 3) ประสิทธิภาพ (Capabilities)



### องค์ประกอบที่ 1 ความตระหนักรู้ (Awareness)

- มิติด้านบุคลากร (People) : ความตระหนักรู้ทำให้บุคลากรมีความรู้เกี่ยวกับหน้าที่ของการกำกับดูแลข้อมูล
- มิติด้านนโยบาย (Policies) : นโยบายการกำกับดูแลข้อมูลมาตรฐานและแนวปฏิบัติที่ดีที่สุดของการกำกับดูแลข้อมูล
- มิติด้านประสิทธิภาพ (Capabilities) : การรู้ถึงสิทธิการเข้าถึงข้อมูลประเภทความสามารถในการควบคุมและพัฒนาให้เกิดคุณค่า

### องค์ประกอบที่ 2 การจัดระเบียบ (Formalization)

- มิติด้านบุคลากร (People) : องค์กรการกำกับดูแลข้อมูลได้รับการพัฒนาอย่างไรและมีบทบาทใดบ้างที่จะสนับสนุนกิจกรรมการกำกับดูแลข้อมูล
- มิติด้านนโยบาย (Policies) : นโยบายการกำกับดูแลข้อมูลมีการกำหนดปฏิบัติและบังคับใช้อย่างเป็นทางการในระดับใด
- มิติด้านประสิทธิภาพ (Capabilities) : การพัฒนาเตรียมพร้อมที่จะทำบางอย่างเพื่อสนับสนุนกิจกรรมการกำกับดูแลข้อมูลและชุดเครื่องมือที่ใช้งานตรวจสอบอย่างสม่ำเสมอ

### องค์ประกอบที่ 3 เมทาดาตา (Metadata)

- มิติด้านบุคลากร (People) : การมีส่วนร่วมในการพัฒนาและบำรุงเมทาดาตา ในระดับใด
- มิติด้านนโยบาย (Policies) : นโยบายการสร้างและบำรุงรักษาเมทาดาตา โดยต้องกำหนดไว้อย่างเป็นทางการ
- มิติด้านประสิทธิภาพ (Capabilities) : การเตรียมจัดการเมทาดาตาที่มีความหลากหลายระดับของการกำกับดูแลข้อมูล

### องค์ประกอบที่ 4 การให้บริการข้อมูล (Stewardship)

- มิติด้านบุคลากร (People) : การทราบถึงข้อมูลที่มีอยู่ที่เกี่ยวกับบทบาทของ Stewardship ในการกำกับดูแลข้อมูล
- มิติด้านนโยบาย (Policies) : นโยบายการกำกับดูแลข้อมูลที่ดีที่สุดต้องทำให้เกิดมาตรฐานและแนวทางปฏิบัติที่ดีที่สุด
- มิติด้านประสิทธิภาพ (Capabilities) : การทราบถึงข้อมูลที่มีความสามารถในการควบคุมข้อมูลที่สามารถสร้างและพัฒนาต่อได้



### องค์ประกอบที่ 5 คุณภาพข้อมูล (Data Quality)

- มิติด้านบุคลากร (People) :** องค์กรที่กำกับดูแลข้อมูลควรได้รับการพัฒนาอย่างไรและมีบทบาทใดที่ตอบสนองและสนับสนุนกิจกรรมของการกำกับดูแลข้อมูล
- มิติด้านนโยบาย (Policies) :** นโยบายการกำกับดูแลข้อมูลมีกำหนดนำไปปฏิบัติและบังคับใช้อย่างเป็นทางการได้ถึงในระดับใด
- มิติด้านประสิทธิภาพ (Capabilities) :** ชุดเครื่องมือที่พัฒนาขึ้นนั้นสนับสนุนกิจกรรมการกำกับดูแลข้อมูลอย่างไรและชุดเครื่องมือนี้จะทำอย่างไรให้เกิดความสม่ำเสมอในการกำกับดูแลข้อมูล

### องค์ประกอบที่ 6 ข้อมูลหลัก (Master Data)

- มิติด้านบุคลากร (People) :** การบริหารจัดการข้อมูลหลักอย่างเป็นทางการนั้นได้รับการพัฒนาได้ถึงระดับใดและได้รับมอบหมายหน้าที่ความรับผิดชอบให้สอดคล้องกันระหว่างข้อมูล
- มิติด้านนโยบาย (Policies) :** นโยบายในการสร้างข้อมูลหลักและการบำรุงรักษาต้องปฏิบัติถึงระดับใดเพื่อการนำไปปฏิบัติและบังคับใช้อย่างเป็นทางการ
- มิติด้านประสิทธิภาพ (Capabilities) :** กำหนดความสามารถในการจัดการเมทาเดตา ในระดับความหลากหลายระดับข้อมูลความเป็นการกำกับดูแลข้อมูล



## 4. การสร้าง การจัดเก็บรักษา การทำลาย และการควบคุมคุณภาพข้อมูล

### 4.1 แนวปฏิบัติการสร้างข้อมูล

- ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัด ในประเด็นดังต่อไปนี้
  - สร้างข้อมูลจากแหล่งข้อมูลต้นทางโดยตรงหรือแหล่งข้อมูลที่น่าเชื่อถือ และอ้างอิง แหล่งที่มาตามรูปแบบที่ถูกต้อง
  - ห้ามสร้างข้อมูลที่บิดเบือน หรือปลอมแปลงไม่ว่าทั้งหมดหรือบางส่วน



### 4.2 แนวปฏิบัติการจัดเก็บข้อมูล

- แนวปฏิบัตินี้หมายความรวมถึง การจัดเก็บข้อมูลทั้งที่เป็นกระดาษ และข้อมูลที่เป็นอิเล็กทรอนิกส์ทุกประเภท ไม่ว่าจะเป็นไฟล์ข้อมูลธรรมดา (Plain Files) ไฟล์ข้อมูลที่มีการเข้ารหัส (Encryption Files) ไฟล์ข้อมูลผ่านการประมวลผล (Information Files) หรือไฟล์ข้อมูลรูปแบบอื่น ๆ
- ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัด ในประเด็นดังต่อไปนี้
  - ต้องจัดเก็บข้อมูลให้ถูกต้องเหมาะสมตามระดับการเปิดเผยข้อมูลของกรมประชาสัมพันธ์ โดยกรมประชาสัมพันธ์ กำหนดระดับการเปิดเผยข้อมูลไว้ดังนี้
    - ข้อมูลสาธารณะ
    - ข้อมูลเปิดเผยในกรมประชาสัมพันธ์
    - ข้อมูลที่ต้องได้รับอนุญาตจากคณะทำงานบริการข้อมูลของกรมประชาสัมพันธ์
    - ข้อมูลที่ต้องได้รับอนุญาตจากหน่วยงานภายนอก
    - ข้อมูลปกปิด
  - การจัดเก็บไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้
    - เจ้าของข้อมูล ผู้สร้างข้อมูลต้องตรวจสอบความถูกต้องของข้อมูลก่อนจัดเก็บ
    - ต้องแจกแจงประเภทของข้อมูลตามลำดับชั้นความลับ รวมถึงกำหนดผู้มีสิทธิในการเข้าถึงหรือควบคุมการใช้งานอย่างเหมาะสม และในกรณีจำเป็นที่ต้องมีการจำกัดการเข้าถึงข้อมูลลับ ให้แก่บุคคลผู้ที่มีหน้าที่เกี่ยวข้อง ให้จัดทำรายชื่อผู้ได้รับอนุญาตให้เข้าถึงดังกล่าวอย่างรอบคอบ
    - เอกสารต้นฉบับต้องได้รับการเก็บรักษาอย่างดีไม่ให้เกิดความเสียหาย

- ต้องป้องกันไฟล์ข้อมูลที่เป็นความลับที่มีการจัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยเครื่องคอมพิวเตอร์ต้องมีการตั้งรหัสผ่านที่มีความมั่นคงปลอดภัย ต้องมีการเข้ารหัสลับ (Encryption) ไฟล์ข้อมูลที่เป็นความลับ
- รหัสผ่านถือเป็นข้อมูลลับและเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษาหัสผ่านให้มีความมั่นคงปลอดภัย

### 4.3 แนวปฏิบัติการทำลายข้อมูล (Data Destruction)

- ต้องมีการตรวจสอบความสอดคล้องของวิธีปฏิบัติการทำลายข้อมูลให้สอดคล้องต่อกฎหมาย นโยบาย และ แนวปฏิบัติที่เกี่ยวข้องกับข้อมูลต้องทำลาย โดยเฉพาะมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ หรือมั่นใจได้ว่า สารสนเทศที่ต้นดูแลรักษาอยู่นั้น ได้ถูกลบทำลายอย่างมั่นคงปลอดภัย เพื่อป้องกันข้อมูลรั่วไหลจากการลักลอบกู้คืนข้อมูล
- การลบทำลายข้อมูลอย่างมั่นคงปลอดภัย ให้ดำเนินการด้วยวิธีการใดวิธีการหนึ่งดังต่อไปนี้
  - ลบทำลายข้อมูลในระดับไฟล์ด้วยวิธีการ Secure Delete
  - ลบทำลายคีย์ไฟล์สำหรับสารสนเทศที่มีการเข้ารหัสลับ (Encrypted Data)
  - ทำลายข้อมูลแบบ Secure Delete/Secure Erase ด้วยวิธีการที่ผู้ผลิตกำหนด
  - ใช้ซอฟต์แวร์ หรือฮาร์ดแวร์สำหรับการลบข้อมูลโดยเฉพาะ (Sanitization)
  - กรณีครุภัณฑ์ หรือส่วนใดส่วนหนึ่งของครุภัณฑ์ของสำนักงานให้ทำลายทิ้งในเชิงกายภาพ เช่น การทำให้เสื่อมภาพของจานแม่เหล็ก (Degauss) บดทำลาย เผาทำลาย โดยต้องผ่านกระบวนการทางพัสดุก่อน
- เมื่อสิ้นสุดการเป็นพนักงานหรือพนักงานโครงการ หรือสิ้นสุดการใช้เครื่องคอมพิวเตอร์ส่วนบุคคล พนักงานหรือพนักงานโครงการมีหน้าที่จะต้องสำรองข้อมูล หรือจะต้องรับผิดชอบข้อมูลด้วยตนเอง พร้อมทั้งดำเนินการส่งเครื่องคอมพิวเตอร์คืนให้แก่หน่วยบริการเทคโนโลยีสารสนเทศ เพื่อดำเนินการทำลายข้อมูลต่อไป
- มีการจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) ของข้อมูลที่ทำลาย เพื่อการตรวจสอบในภายหลัง
- ต้องมีการจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนคุม และบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี



## 4.4 แนวปฏิบัติการควบคุมคุณภาพข้อมูล (Data Quality)

### หลักการการจัดการคุณภาพของข้อมูล (Data Quality Principles)

คุณภาพของข้อมูล (Data Quality) คือ ข้อมูลที่ดีได้มาตรฐานตามที่กำหนด กล่าวคือ ผลรวมของคุณลักษณะและคุณสมบัติของผลิตผลข้อมูลที่พึงประสงค์ทุกประการของผลการปฏิบัติงานตามดัชนีตัวชี้วัดคุณภาพและองค์ประกอบที่กำหนดไว้ ข้อมูลที่เหมาะสมกับการใช้งาน ตอบสนองต่อความต้องการที่กำหนด และตรงตามวัตถุประสงค์

การกำหนดแกนหลักในการขับเคลื่อนแนวทางในการกำกับดูแลคุณภาพของข้อมูล ประกอบด้วยหลักการ 7 ประการ ดังนี้

- **หลักการที่ 1:** การกำกับดูแลข้อมูลที่มีประสิทธิภาพกำหนดให้ต้องวัดผล และทำความเข้าใจข้อมูลขององค์กร โดยกรมประชาสัมพันธ์จะกำหนดมาตรการและมาตรวัดเพื่อประเมินประสิทธิภาพการจัดการข้อมูล
- **หลักการที่ 2:** ระบบอัตโนมัติจำเป็นอย่างยิ่งในการขยายคุณภาพข้อมูลทั่วทั้งกรมประชาสัมพันธ์ หากเป็นไปได้ กรมประชาสัมพันธ์ควรลงทุนในกระบวนการและเครื่องมือเพื่อช่วยให้กิจกรรมด้านคุณภาพข้อมูลเป็นไปโดยอัตโนมัติ
- **หลักการที่ 3:** กรมประชาสัมพันธ์ต้องลดความซับซ้อนของสภาพแวดล้อมข้อมูล โดยกรมประชาสัมพันธ์จะต้องพยายามใช้แหล่งข้อมูลที่เป็นทางการเท่านั้น และในขณะเดียวกันต้องทำการพิจารณาการยกเลิกการใช้แหล่งข้อมูลที่ไม่เป็นทางการ
- **หลักการที่ 4:** ความเข้าใจเรื่องคุณภาพของข้อมูลที่กรมประชาสัมพันธ์ได้รับ มีความจำเป็นต่อการใช้ข้อมูลอย่างมีประสิทธิภาพ ไม่ว่าข้อมูลจะมีคุณภาพสูงหรือต่ำ กรมประชาสัมพันธ์ต้องประเมินและรับทราบผลกระทบที่อาจมีต่อภารกิจขององค์กร
- **หลักการที่ 5:** ความซับซ้อนในการออกแบบเป็นอุปสรรคต่อความสามารถในการรักษาข้อมูลคุณภาพสูง กรมประชาสัมพันธ์จำเป็นต้องดำเนินการวางแผนผังข้อมูล (Data Map) และการจำแนก Data Domains เพื่อจัดโครงสร้างวิธีการจำลองข้อมูล
- **หลักการที่ 6:** การดำเนินการด้านคุณภาพข้อมูลจะมุ่งเน้นไปที่วิธีเปิดใช้งานข้อมูลที่เป็นของกรมประชาสัมพันธ์ กฎคุณภาพข้อมูลควรซับซ้อนเท่าที่จำเป็น
- **หลักการที่ 7:** การเก็บรักษาและการทำซ้ำข้อมูลทำให้รักษาข้อมูลคุณภาพสูงได้ยากขึ้น กรมประชาสัมพันธ์ควรเก็บรักษาและทำซ้ำข้อมูลเมื่อจำเป็นต้องใช้ข้อมูลดังกล่าว เพื่อเปิดใช้งานกรณีการใช้งานเฉพาะ



## มาตรฐานด้านคุณภาพของข้อมูล (Data Quality Standard)

### มิติของแบบจำลองคุณภาพข้อมูล

กรมประชาสัมพันธ์ต้องตกลงร่วมกันในคำจำกัดความของคุณภาพของข้อมูล โดยการสร้างแบบจำลองคุณภาพของข้อมูลในหลายมิติ แต่ละมิติควรระบุลักษณะความต้องการของแต่ละหน่วยงาน และความตั้งใจที่จะใช้ข้อมูลในกรณีการใช้งานจากมุมมองเชิงปฏิบัติ กรอบผลลัพธ์ต้องสนับสนุนการประเมินคุณภาพข้อมูล โดยอ้างอิงกรอบคุณภาพข้อมูลดังต่อไปนี้

- กรมประชาสัมพันธ์จะใช้มิติและมาตรการในกรอบคุณภาพข้อมูลเพื่อสร้างแบบจำลองของคุณภาพของข้อมูล
- Data Quality Lead จะต้องประสานงานกับ Data Stewards เพื่อระบุเป้าหมายด้านคุณภาพข้อมูลสำหรับแต่ละมิติในระดับโดเมนย่อยของข้อมูลและโดยรวม

มิติ (Dimension)	คำอธิบาย	มาตรการชี้วัด	เป้าหมาย
ความถูกต้อง Accuracy	รายการตรงกับแหล่งที่มาที่ตกลงไว้หรือไม่	% ของรายการที่มีค่าไม่ถูกต้อง (เช่น ที่อยู่ทางไปรษณีย์ล้าสมัย)	80%
ความสอดคล้องกัน Consistency	องค์ประกอบข้อมูลแต่ละรายการมีแหล่งข้อมูลที่เป็นทางการแหล่งเดียวหรือไม่	% ขององค์ประกอบข้อมูลที่ไม่มีแหล่งที่มาอย่างเป็นทางการ	70%
ความสมบูรณ์ Completeness	มีการเติมฟิลด์ที่จำเป็นทั้งหมดหรือไม่	% ของฟิลด์ที่ต้องกรอกไม่สมบูรณ์หรือไม่ได้เติมข้อมูล	80%
ความเป็นเอกลักษณ์ Uniqueness	บันทึกถูกจัดเก็บไว้ในที่เก็บข้อมูลเดียวและไม่ซ้ำกันสำหรับลูกค้าแต่ละรายหรือไม่	% ของเรคคอร์ดที่ทำซ้ำในที่เก็บข้อมูลหนึ่งหรือซ้ำกับลูกค้า	75%
ความเป็นปัจจุบัน Timeliness	องค์ประกอบข้อมูลได้รับการเฟรชในเวลาที่เหมาะสมหรือไม่?	% ของเวลาที่องค์ประกอบข้อมูลไม่ได้รับการรีเฟรชเพียงพอที่จะเปิดใช้งานกรณีการใช้งาน	85%
ความพร้อมใช้ Availability	รายการในรูปแบบปัจจุบันของข้อมูลในอดีตสามารถเข้าถึงได้แบบดิจิทัลหรือไม่	% ของรายการเวลา ทั้งในรูปแบบปัจจุบันหรือในอดีต ไม่สามารถเข้าถึงได้	80%
การตีความ Interpretability	แต่ละรายการมีคำจำกัดความและที่มาที่ชัดเจนหรือไม่	% ของแอตทริบิวต์ metadata ที่ไม่ได้กำหนดไว้ใน data dictionary	90%
ความเที่ยงตรง Validity	ค่าในชุดข้อมูลถูกจำกัดโดยกฎทางธุรกิจหรือไม่	% ขององค์ประกอบข้อมูลในชุดข้อมูลที่ถูกลimit	85%

คุณภาพของข้อมูล คือข้อมูลที่ได้รับการประเมินในระดับโดเมนย่อยโดย Platform Steward และ Data Quality Lead ที่เหมาะสม

รูปที่ 3 Data Quality Framework

### การประเมินคุณภาพข้อมูล

กรมประชาสัมพันธ์ควรประเมินระดับคุณภาพข้อมูลเป็นระยะ เพื่อตอบสนองต่อเหตุการณ์ต่าง ๆ รวมทั้งการประเมินเป็นระยะจะให้ข้อมูลที่จำเป็นในการปรับปรุงคุณภาพข้อมูลเมื่อเวลาผ่านไปสามารถนำไปใช้กับกรณีการใช้งานต่าง ๆ ได้อย่างง่ายดาย การประเมินตามเหตุการณ์จะช่วยให้กรมประชาสัมพันธ์สามารถวัดคุณภาพของข้อมูลที่ได้มาใหม่ หรือสร้างขึ้นได้ ซึ่งการประเมินคุณภาพของข้อมูลต้องได้รับการสนับสนุนจากผู้บริหารจัดการข้อมูล เพื่อบังคับใช้การตรวจสอบคุณภาพของข้อมูล

- Data Quality Lead ต้องบังคับใช้กระบวนการเพื่อให้แน่ใจว่าหน่วยงานจัดทำโปรไฟล์โดเมนย่อยข้อมูลใหม่ รวมถึงการประเมินคุณภาพข้อมูล เมื่อมีการกำหนดเนื่องจากการสร้างข้อมูลใหม่หรือการนำเข้าข้อมูลใหม่จากบุคคลที่สาม
- Data Quality Lead ต้องบังคับใช้กระบวนการเพื่อให้แน่ใจว่าหน่วยงานต่าง ๆ จะประเมินคุณภาพข้อมูลของ Data Subdomain ผ่านการสุ่มตัวอย่างอย่างน้อยปีละ 2 ครั้ง

- เจ้าของข้อมูลต้องตรวจสอบให้แน่ใจว่าข้อมูลส่วนบุคคลนั้นถูกต้อง เป็นปัจจุบัน ครบถ้วน และไม่ก่อให้เกิดความเข้าใจผิดตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)

กรมประชาสัมพันธ์ควรมิติข้อมูลตามกรอบคุณภาพข้อมูล (Data Quality Framework) เพื่อประเมินระดับคุณภาพข้อมูลสำหรับแต่ละ Data Subdomain :

- Data Quality Lead จะใช้เกณฑ์คุณภาพข้อมูลเพื่อให้คะแนนคุณภาพข้อมูลสำหรับแต่ละ Data Subdomain และคำนวณคะแนนคุณภาพข้อมูลขั้นสุดท้าย
- Data Quality Lead จะต้องตกลงน้ำหนัก (Weight) สำหรับแต่ละมิติของกรอบคุณภาพข้อมูลกับ Data Steward สำหรับแต่ละ Data Subdomain เพื่อสะท้อนให้เห็นว่าข้อมูลนั้น ถูกใช้ โดยหน่วยงาน
- Data Quality Lead จะใช้วิธีการสุ่มตัวอย่างเพื่อตรวจสอบองค์ประกอบข้อมูลและประเมินคุณภาพข้อมูลสำหรับแต่ละ Data Subdomain
- Data Quality Lead จะต้องประสานงานกับเจ้าของข้อมูลเพื่อให้กระบวนการประเมินคุณภาพข้อมูลเป็นแบบอัตโนมัติในขอบเขตที่เป็นไปได้
- Data Quality Lead จะต้องประสานงานกับ Platform Stewards เพื่อยกระดับ Data Subdomains ด้วยคะแนนคุณภาพข้อมูลขั้นสุดท้ายเท่ากับสอง (2) หรือต่ำกว่า
- Data Stewards จะประสานงานกับ Data Quality Lead เพื่อทำความเข้าใจบริบททางธุรกิจของข้อมูล ระบุองค์ประกอบข้อมูลที่สำคัญ และอุปกรณ์การวัดที่เหมาะสมสำหรับมิติข้อมูลคุณภาพ (เช่น กำหนดสิ่งที่ประกอบขึ้นเป็นชุดข้อมูล)

Dimension	Measure	คะแนนคุณภาพข้อมูล				
		80%+	60%+	40%+	20%+	0%+
ความถูกต้อง Accuracy	▪ % ของรายการที่มีค่าไม่ถูกต้อง (เช่น ที่อยู่ทางไปรษณีย์ ล้าสมัย)	1	2	3	4	5
ความสอดคล้องกัน Consistency	▪ % ขององค์ประกอบข้อมูลที่ไม่มีแหล่งที่มาอย่างเป็นทางการ	1	2	3	4	5
ความสมบูรณ์ Completeness	▪ % ของฟิลด์ที่ต้องกรอกไม่สมบูรณ์หรือไม่ได้เติมข้อมูล	1	2	3	4	5
ความเป็นเอกลักษณ์ Uniqueness	▪ % ของเรกคอร์ดที่ซ้ำกันในที่เก็บข้อมูลหนึ่งหรือซ้ำกับลูกค้า	1	2	3	4	5
ความเป็นปัจจุบัน Timeliness	▪ % ของเวลาที่องค์ประกอบข้อมูลไม่ได้รับการรีเฟรชพอที่จะเปิดใช้งานกรณีการใช้งาน	1	2	3	4	5
ความพร้อมใช้ Availability	▪ % ของรายการเวลา ทั้งในรูปแบบปัจจุบันหรือในอดีต ไม่สามารถเข้าถึงได้	1	2	3	4	5
การตีความ Interpretability	▪ % ของแอตทริบิวต์ metadata ที่ไม่ได้กำหนดไว้ใน data dictionary	1	2	3	4	5
ความเที่ยงตรง Validity	▪ % ขององค์ประกอบข้อมูลในชุดข้อมูลที่ถูกต้อง	1	2	3	4	5

คะแนนคุณภาพข้อมูลขั้นสุดท้ายคือคะแนนค่าสุดท้ายของการให้คะแนนแต่ละมิติ

รูปที่ 4 Data Quality Thresholds



## การแก้ไขปัญหาคุณภาพข้อมูล

คะแนนคุณภาพข้อมูลต่ำ หมายความว่า ข้อมูลที่หน่วยงานนั้นยังบกพร่องในกรอบคุณภาพข้อมูล ตั้งแต่หนึ่งมิติขึ้นไป ซึ่งส่งผลเสียต่อความสามารถในการใช้งานของข้อมูลและลดทอนความสามารถของหน่วยงานในการประมวลผลหรือแบ่งปันข้อมูล เพื่อแก้ไขปัญหาและจึงควรทำให้แน่ใจว่าข้อมูลได้รับการจัดการในลักษณะที่ปรับการใช้งานให้เหมาะสม กรมประชาสัมพันธ์ควรแก้ไขโดเมนย่อยข้อมูลที่มีคะแนนคุณภาพข้อมูลต่ำ ในทำนองเดียวกันควรประเมินและแก้ไขรายงานปัญหาคุณภาพข้อมูล

- Data Stewards ยกระดับโดเมนย่อยของข้อมูลที่ควรได้รับการแก้ไขไปยังผู้บริหารฝ่ายจัดการข้อมูล โดเมนย่อยข้อมูลที่มีคะแนนคุณภาพข้อมูลสอง (2) หรือต่ำกว่าควรได้รับการแก้ไขใหม่
- Platform Stewards วิเคราะห์โดเมนย่อยข้อมูลที่ได้รับการเลื่อนระดับเพื่อระบุปัญหาด้านคุณภาพข้อมูลที่ส่งผลให้คะแนนคุณภาพข้อมูลเป็นสอง (2) หรือต่ำกว่า
- Data Quality Lead จะต้องประเมินปัญหาคุณภาพข้อมูลที่ระบุและปัญหาที่พนักงานรายงานสำหรับความรุนแรงตามตัวเลขความรุนแรงของปัญหาคุณภาพข้อมูล และจัดลำดับความสำคัญของปัญหาคุณภาพข้อมูลที่จะวิเคราะห์

ระดับความรุนแรง		
ระดับความรุนแรงต่ำ (Low Severity)	ระดับความรุนแรงปานกลาง (Medium Severity)	ระดับความรุนแรงสูง (High Severity)
<b>ขอบเขตของปัญหา</b> <ul style="list-style-type: none"> <li>แต่ละแผนกภายในหน่วยงาน</li> </ul>	<ul style="list-style-type: none"> <li>หน่วยงานทั้งหมด</li> </ul>	<ul style="list-style-type: none"> <li>ทั้งกรมประชาสัมพันธ์ หรือแต่ละหน่วยงาน</li> </ul>
<b>การมีส่วนร่วมของผู้มีส่วนได้ส่วนเสีย</b> <ul style="list-style-type: none"> <li>ปัญหาต้องมีการดำเนินการแก้ไขโดยเจ้าหน้าที่ระดับปฏิบัติการ</li> </ul>	<ul style="list-style-type: none"> <li>ปัญหาที่ต้องได้รับความสนใจจากฝ่ายบริหาร ได้แก่ หัวหน้าหน่วยงาน</li> </ul>	<ul style="list-style-type: none"> <li>ปัญหาที่ต้องให้ความสนใจจากคณะกรรมการควบคุมการกำกับดูแลข้อมูล (Data Governance Steering Committee)</li> </ul>

รูปที่ 5 Data Quality Issue Severity

- Platform Stewards จะประสานงานกับผู้บริหารฝ่ายจัดการข้อมูลเพื่อทำการวิเคราะห์สาเหตุของปัญหาด้านคุณภาพของข้อมูลที่จัดลำดับความสำคัญ และระบุสาเหตุที่เกิดปัญหาด้านคุณภาพของข้อมูล
- Data Quality Lead จะต้องจัดหมวดหมู่ปัญหาด้านคุณภาพข้อมูลตามสาเหตุที่แท้จริง โดยการใช้การจำแนกของปัญหาด้านคุณภาพข้อมูล



Data entry & conversion causes	Data conversion	ข้อมูลถูกปฏิเสธหรือข้อมูลผิดประเภทหลังจากการแปลงข้อมูล เนื่องจากข้อมูลไม่เพียงพอเกี่ยวกับการตีความแหล่งข้อมูล ข้อมูลต้นฉบับอาจผิดพลาดได้
	System consolidation	ข้อมูลใหม่ที่ไม่เข้ากับโครงสร้างที่มีอยู่ การทับซ้อนของข้อมูล ความขัดแย้งของข้อมูล
	Manual data entry	ข้อผิดพลาดเกิดขึ้นเนื่องจากขาดสมาธิหรือแรงจูงใจ พิมพ์ผิด มีการเว้นช่องว่าง กรอกข้อมูลซ้ำเริ่มต้น
	Batch/ETL feeds	การเปลี่ยนแปลงโครงสร้างของโครงสร้างต้นทาง ไม่ใส่ใจข้อผิดพลาดในโปรแกรม
	Real-time interfaces	ข้อมูลที่มีเส้นทางใหม่จะต้องได้รับการยอมรับหรือปฏิเสธจากฐานข้อมูลทันที ข้อมูลที่ถูกต้องและเป็นข้อมูลที่ถือว่าสูญหาย ข้อมูลที่ไม่ถูกต้องอาจแพร่กระจายด้วยวิธีนี้
Direct causes	Data processing	การเปลี่ยนแปลงโปรแกรมเล็กน้อยอาจส่งผลให้เกิดความไม่สอดคล้องกัน ข้อมูลถูกแปลงและไม่สอดคล้องกับโครงสร้างฐานข้อมูล (DB)
	Data cleansing	ปัญหาด้านคุณภาพของข้อมูลมีความซับซ้อนและเกี่ยวเนื่องกัน การแก้ไขปัญหาหนึ่งอาจสร้างปัญหาอื่น ๆ อีกมากมายในองค์ประกอบข้อมูลเดียวกันหรืออื่น ๆ ที่เกี่ยวข้องกัน
	Data purging	โครงสร้างข้อมูลเปลี่ยนแปลงและเมื่อข้อมูลถูกกำจัด มีความเสี่ยงที่ข้อมูลที่เกี่ยวข้องบางอย่างจะถูกลบโดยไม่ได้ตั้งใจ
Indirect causes	Changes not captured	ข้อมูลวัตถุ หรือข้อมูลส่วนบุคคลจริงอาจมีการเปลี่ยนแปลงข้อมูล (เช่น เจ้าของข้อมูลเสียชีวิต) ดังนั้นข้อมูลดังกล่าวจึงเกิดความผิดพลาด
	Systems upgrades	ฟิลด์ข้อมูลถูกใช้เพื่อวัตถุประสงค์ที่ไม่ถูกต้อง และข้อมูลบางส่วนหายไป ในขณะที่ข้อมูลอื่น ๆ ถูกทำให้อยู่ในรูปแบบที่โปรแกรมเวอร์ชันก่อนหน้ายอมรับได้
	New data uses	ข้อมูลอาจดีเพียงพอสำหรับวัตถุประสงค์หนึ่ง แต่ไม่เพียงพอสำหรับวัตถุประสงค์หนึ่ง การใช้งานใหม่อาจเพิ่ม ให้ความสำคัญกับความต้องการข้อมูลมากขึ้น แม้จะไม่ได้เปลี่ยนคำจำกัดความของคุณภาพก็ตาม
	Loss of expertise	ความรู้ด้านข้อมูลส่วนใหญ่อยู่ในสเกิล หรือความรู้ของพนักงาน เจ้าหน้าที่ มากกว่าเอกสาร Metadata เมื่อพนักงาน เจ้าหน้าที่เหล่านี้มีการโยกย้าย ลากออก เกษียณอายุ ข้อมูลจะไม่ถูกใช้ซ้ำอีกต่อไป
	Process automation	พนักงาน เจ้าหน้าที่ มีการตรวจสอบข้อมูลโดยอัตโนมัติก่อนใช้งาน ส่วนโปรแกรมคอมพิวเตอร์ใช้ข้อมูลจริงที่ไม่ผ่านการตรวจสอบ และไม่สามารถตัดสินใจอย่างเหมาะสมเกี่ยวกับความเป็นไปได้ที่ข้อมูลนั้นจะถูกต้อง

รูปที่ 6 Data Quality Issue Category

- ปัญหาด้านคุณภาพข้อมูลที่เกิดจากข้อผิดพลาดในการป้อนข้อมูลหรือการแปลง Data Stewards จะต้องบังคับใช้กฎด้านคุณภาพข้อมูลสำหรับฟิลด์ข้อมูลที่ได้รับผลกระทบ เพื่อให้แน่ใจว่าข้อผิดพลาดนี้จะไม่เกิดขึ้นอีกในอนาคต
- คุณภาพของข้อมูลที่เกิดจากการป้อนข้อมูลหรือข้อผิดพลาดในการแปลงข้อมูล Platform Stewards ต้องออกแบบและใช้การควบคุมทางเทคนิคเพื่อบังคับใช้กฎคุณภาพข้อมูลที่กำหนดโดย Data Stewards
- กฎคุณภาพข้อมูลจะใช้ข้อกำหนดทางธุรกิจเพื่อจำกัดองค์ประกอบข้อมูลให้อยู่ในชุดของค่าที่คาดไว้
- ปัญหาด้านคุณภาพข้อมูลที่เกิดจากการป้อนข้อมูลหรือข้อผิดพลาดในการแปลงข้อมูล Data Quality Lead จะต้องจัดทำเอกสารกฎคุณภาพข้อมูลที่สร้างขึ้นสำหรับแต่ละโดเมนย่อยของข้อมูล และยอมรับเงื่อนไขการทดสอบซ้ำโดยใช้รูปแบบ เช่น เทมเพลตกฎคุณภาพข้อมูลดังต่อไปนี้

องค์ประกอบข้อมูล Data Element		กฎทางธุรกิจ Business Rule		มาตรการชี้วัด Measure					
Data domain	Data subdomain	คำอธิบายขององค์ประกอบข้อมูล	พริกเกอร์หรือข้อควรระวังในการทดสอบ	ประเมินรายการข้อมูลทั้งหมด	รายการข้อมูลทั้งหมดที่ไม่ถูกต้อง	% ของการป้อนข้อมูลไม่ถูกต้อง	เกณฑ์การยอมรับ %	Target date	
สำนักพัฒนาการประชาสัมพันธ์	ข้อมูลบัตรประชาชนประจำตัวประชาชน	ID Card Number	แสดงเฉพาะ: พารามิเตอร์ประจำตัวประชาชนมีจำนวนตัวไม่เกิน 11	ID_Card_No > 11    ID_Card_No < 11	10,024	11	0.1 %	0.15 %	20230521
สำนักพัฒนาการประชาสัมพันธ์	ข้อมูลประเภทการฝึกอบรม	Training Course Type	แสดงเฉพาะ: ข้อมูลประเภทการฝึกอบรมไม่ตรงกับประเภทการฝึกอบรมที่ผู้จัด	Training_Course_type != ("Onsite"    "Online"    "Workshop"    "Seminar")	17,365	2379	13.6 %	20%	20230501
สำนักพัฒนาการประชาสัมพันธ์	ข้อมูลการลงทะเบียน	Register	แสดงเฉพาะ: ข้อมูลการลงทะเบียนสำเร็จไม่เป็นจริงหรือเป็นเท็จ	Register != ("True"    "False")	1,735	68	4 %	5 %	20230331

รูปที่ 7 Data Quality Rules Template



## การจัดการแหล่งข้อมูลอย่างเป็นทางการ

ปัญหาด้านคุณภาพของข้อมูลจำนวนมากเกิดขึ้น เนื่องจากการใช้ข้อมูลจากแหล่งข้อมูลที่ไม่เป็นทางการ ในฐานะส่วนหนึ่งของการรับประกันคุณภาพของข้อมูลในกรมประชาสัมพันธ์ ผู้บริหารฝ่ายการจัดการข้อมูลควรสนับสนุนให้ธุรกิจใช้ข้อมูลจากแหล่งข้อมูลที่เป็นทางการ ซึ่งดูแลโดย Platform Stewards ที่ได้รับการยอมรับเท่านั้น

- เจ้าของข้อมูล (Data Owner) ต้องประสานงานกับผู้บริหารฝ่ายจัดการข้อมูลเพื่อกำหนดแผนการยกเลิกการใช้แหล่งข้อมูลที่ไม่เป็นทางการ และลดความซับซ้อนของสภาพแวดล้อมข้อมูลในกรมประชาสัมพันธ์อย่างต่อเนื่อง
- Platform Stewards ต้องประสานงานกับผู้บริหารฝ่ายจัดการข้อมูลเพื่อให้แน่ใจว่าระบบประมวลผลข้อมูลที่ใช้ในการจัดเก็บและประมวลผลข้อมูลได้รับการออกแบบมาเพื่อรองรับมิติของคุณภาพข้อมูล



## 5. การประมวลผลและ การใช้ข้อมูล

### 5.1 แนวปฏิบัติการประมวลผลข้อมูล

- ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัดในประเด็นดังต่อไปนี้
  - ต้องปฏิบัติตามขั้นตอนการประมวลผลข้อมูลและการใช้ข้อมูลที่กำหนดขึ้น เพื่อให้มีสิทธิการใช้งานระบบสารสนเทศตามความจำเป็น
  - ต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำไปประมวลผล
  - กรณีข้อมูลมีการควบคุมโดยการเข้ารหัส (Encryption) ในการประมวลผลข้อมูลต้องบันทึกหลักฐานไว้ทุกครั้งเพื่อการตรวจสอบในภายหลัง และสามารถจัดพิมพ์เป็นรายงานเพื่อการตรวจสอบได้
  - ต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการประมวลผลข้อมูลที่ได้กำหนดขึ้นข้อมูลตั้งแต่กลับขึ้นไปอย่างเพียงพอและมีประสิทธิภาพ

### 5.2 5.1 แนวปฏิบัติการใช้ข้อมูล

- ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัดในประเด็นดังต่อไปนี้
  - ให้ใช้ข้อมูลทั้งที่มีอยู่ภายในหน่วยงาน หรือได้รับข้อมูลจากภายนอกหน่วยงานเพื่องานในราชการเท่านั้น
  - ใช้ข้อมูลเฉพาะในส่วนที่ได้รับอนุญาตตามการกำหนดสิทธิจากผู้ดูแลระบบคอมพิวเตอร์ เท่านั้น
  - กรณีข้อมูลที่มีความสำคัญหรือชั้นความลับ ต้องมีการกำหนดสิทธิผู้ใช้งานและสิทธิในการเข้าถึง ระยะเวลาที่นำข้อมูลไปใช้งาน วัตถุประสงค์ในการใช้งานข้อมูล
  - ห้ามมิให้ใช้ข้อมูลเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว หรือใช้ข้อมูลอันอาจก่อให้เกิดความเสียหายต่อหน่วยงาน



## 6. การเปิดเผยข้อมูล/การเชื่อมโยง

- ต้องปฏิบัติตามกฎหมาย ระเบียบ ประกาศ และหลักเกณฑ์ที่เกี่ยวข้อง และให้ปฏิบัติโดยเคร่งครัดในประเด็นดังต่อไปนี้
  - ข้อมูลมีความพร้อมในการส่งต่อหรือเปิดเผยได้ ข้อมูลที่เปิดเผยควรเป็น Open by Default และ Closed by Exception โดย Open by Default จะเป็นลักษณะของข้อมูลที่สามารถเปิดเผยได้และไม่ละเมิดข้อมูลส่วนบุคคล เช่น ข้อมูลเชิงสถิติที่ไม่มีตัวบุคคล ในส่วน Closed by Exception เป็นลักษณะข้อมูลส่วนบุคคลที่ไม่ควรเปิดเผย เช่น หมายเลขบัตรประจำตัวประชาชน หมายเลขบัตรเครดิต รหัสผ่านที่ใช้เข้าระบบ เป็นต้น
  - ต้องมีการตรวจสอบชั้นความลับของข้อมูล (Data Classification) ว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่
  - กรณีข้อมูลที่เป็นความลับ หากจำเป็นต้องแลกเปลี่ยนข้อมูลหน่วยงานปลายทางจะต้องมีการจัดทำธรรมาภิบาลข้อมูลในระดับเดียวกัน หากไม่มีการจัดทำธรรมาภิบาลข้อมูลต้องมีการทำสัญญาอนุญาตหรือเงื่อนไขในการแลกเปลี่ยน และการนำข้อมูลไปใช้ที่ยอมรับได้ ห้ามนำไปเผยแพร่ต่อโดยเด็ดขาด
  - ต้องมีการเข้ารหัสลับ (Encryption) ข้อมูลก่อนการแลกเปลี่ยนข้อมูลบางประเภท เช่น ข้อมูลความมั่นคงประเทศ
  - ข้อมูลส่วนบุคคลบางรายการต้องไม่แสดงตัวตน (Anonymization) กรณีที่หน่วยงานที่ขอข้อมูลไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูลเพื่อทำการศึกษาหรือวิจัย
  - มีกลไกตรวจสอบให้แน่ใจว่าการแลกเปลี่ยนข้อมูลถูกดำเนินการได้อย่างเหมาะสมหรือเป็นไปตามแนวปฏิบัติ กระบวนการแลกเปลี่ยน และมาตรฐานที่กำหนด

