บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)
National Telecom Public Company Limited

ประกาศ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

เรื่อง นโยบายและแนวปฏิบัติการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่

(Data Governance and Big Data Management)

เพื่อให้การกำหนด สิทธิ หน้าที่ และความรับผิดชอบในการดำเนินงานเกี่ยวกับข้อมูล ที่สนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้น รวมทั้งป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูลที่จะส่งผลให้เกิดความเสียหายต่อการดำเนินธุรกิจของบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ตลอดจนสร้างความมั่นใจให้กับผู้มีส่วนได้ส่วนเสียเกี่ยวกับความมั่นคงปลอดภัยของข้อมูล การรักษาความเป็นส่วนบุคคลที่เป็นไปตามมาตรการในการกำกับดูแลข้อมูล (Data Governance)

อาศัยอำนาจตามความในข้อ 2.1 ของคำสั่งคณะกรรมการบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ที่ 3/2564 เรื่อง มอบอำนาจให้กรรมการผู้จัดการใหญ่ปฏิบัติการแทนคณะกรรมการบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) จึงประกาศให้ใช้นโยบายและแนวปฏิบัติการกำกับดูแลข้อมูล และการบริหารจัดการข้อมูลขนาดใหญ่ (Data Governance and Big Data Management) ตามที่แนบท้ายประกาศนี้

จึงประกาศเพื่อทราบและถือปฏิบัติ

ประกาศ ณ วันที่ 4 มกราคม 2566

พันเอก (signature)

(สรรพชัยย์ หุวะนันทน์)

กรรมการผู้จัดการใหญ่

นโยบายและแนวปฏิบัติการกำกับดูแลข้อมูล และการบริหารจัดการข้อมูลขนาดใหญ่

(Data Governance and Big Data Management)

แนบท้ายประกาศบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

วัตถุประสงค์

เพื่อกำหนด สิทธิ หน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องในการกำกับดูแลและบริหารจัดการข้อมูล ที่จะช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้น รวมทั้งป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูลที่จะส่งผลให้เกิดความเสียหายต่อการดำเนินธุรกิจของ บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ตลอดจนสร้างความมั่นใจให้กับผู้มีส่วนได้ส่วนเสียเกี่ยวกับความมั่นคงปลอดภัยของข้อมูล การรักษาความเป็นส่วนบุคคลที่เป็นไปตามมาตรการในการกำกับดูแลข้อมูลที่ดี (Data Governance) จึงกำหนดนโยบายและแนวปฏิบัติการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ เพื่อเป็นแนวทางให้ผู้บริหาร ผู้ปฏิบัติงาน และบุคคลภายนอกถือปฏิบัติได้อย่างถูกต้องเหมาะสม

เพื่อให้การจัดการข้อมูลที่มีอยู่และข้อมูลขนาดใหญ่ในอนาคตที่จะเกิดขึ้นมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มีประสิทธิภาพ และมั่นคงปลอดภัย สามารถนำไปใช้ในการวิเคราะห์ ประมวลผลเพื่อการตัดสินใจอย่างแม่นยำ มีประสิทธิภาพมากยิ่งขึ้น สอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของบริษัท -บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) จึงกำหนดนโยบายและแนวปฏิบัติการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ ดังนี้

1. คำจำกัดความ

1.1 คณะกรรมการกำกับดูแลข้อมูล (Data Governance Council) หมายถึง คณะทำงานซึ่งประกอบด้วย ผู้บริหารระดับสูง ระดับรองกรรมการผู้จัดการใหญ่ด้าน CIO, CDO, CSO เป็นต้น

1.2 ทีมบริกรข้อมูล (Data Steward Team) หมายถึง กลุ่มผู้ปฏิบัติงานที่ทำหน้าที่สนับสนุนในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ ประกอบด้วย หัวหน้าทีมบริกรข้อมูล (Lead Data Steward) บริกรข้อมูลด้านธุรกิจ (Buslness Data Stewards) บริกรข้อมูลด้านเทคนิค (Technical Data Stewards) บริกรข้อมูลด้านคุณภาพข้อมูล (Data Quality Stewards) รวมไปถึงผู้ปฏิบัติงานที่ทำหน้าที่เกี่ยวกับความมั่นคงปลอดภัย และกฎหมาย

1.3 ทีมบริหารจัดการข้อมูล (Data Management Team) หมายถึง กลุ่มผู้ปฏิบัติงานที่ทำหน้าที่บริหารจัดการข้อมูล ประกอบด้วย สถาปนิกข้อมูล (Data Architects) วิศวกรข้อมูล (Data Engineer)

นักจัดการฐานข้อมูล (Database Administrators - DBA) นักวิเคราะห์ข้อมูล (Data Analysts) และ นักวิทยาการข้อมูล (Data Scientists)

1.4 เจ้าของข้อมูล (Data Owners) หมายถึง ผู้ปฏิบัติงานแต่ละฝ่ายที่ทำหน้าที่ดูแลข้อมูลให้สอดคล้องกับ นโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย

1.5 ผู้สร้างข้อมูล (Data Creators) หมายถึง ผู้ปฏิบัติงานที่ทำหน้าที่เกี่ยวกับข้อมูลตามโครงสร้างที่ถูกกำหนดไว้

1.6 ผู้ใช้ข้อมูล (Data Users) หมายถึง ผู้ปฏิบัติงานหรือบุคคลภายนอกที่นำข้อมูลไปใช้งานทั้งระดับปฏิบัติงานและระดับบริหาร

1.7 ข้อมูล หมายถึง ข้อเท็จจริงหรือเรื่องราวที่เกี่ยวกับสิ่งต่าง ๆ โดยอยู่ในรูปแบบที่เหมาะสมต่อการสื่อสาร การแปลความหมายและการประมวลผล เช่น ข้อมูลส่วนบุคคล ข้อมูลลูกค้า ข้อมูลทางธุรกิจ และข้อมูลของบริษัททั้งที่อยู่ภายในและนอกระบบคอมพิวเตอร์ของบริษัท เป็นต้น

1.8 เมทาดาตา (Metadata) หมายถึง นิยาม คำอธิบาย รายละเอียด และคุณลักษณะโครงสร้างของข้อมูล

2. ประเภทข้อมูล (Data Policy)

ส่วนงานเจ้าของข้อมูลมีหน้าที่แบ่งประเภทของข้อมูลเพื่อสะดวกในการบริหารจัดการข้อมูลในส่วนที่เกี่ยวข้องต่อไป โดยแบ่งข้อมูลเป็นประเภทดังนี้

2.1 ข้อมูลที่มีโครงสร้าง (Structure Data) เป็นข้อมูลที่มีนิยามโครงสร้างของข้อมูล โดยมีความหมายและคุณสมบัติของแต่ละฟิลด์ข้อมูล โครงสร้างมีชั้นเดียว ง่ายต่อการค้นหา เช่น ตารางข้อมูลในฐานข้อมูลไฟล์ประเภท Comma-Separated Values – CSV เป็นต้น

2.2 ข้อมูลกึ่งโครงสร้าง (Semi-structure Data) เป็นข้อมูลที่มีนิยามโครงสร้างของข้อมูล แต่มีโครงสร้างเป็นแบบลำดับขั้น (Hierarchy) เช่น ข้อมูลที่อยู่ในรูปแบบ Extensible Markup Language - XM หรือ JavaScript Object Notation - JSON เป็นต้น

2.3 ข้อมูลไม่มีโครงสร้าง (Unstructured Data) เป็นข้อมูลที่ไม่มีนิยามโครงสร้าง ซึ่งจะอยู่ในรูปแบบ เช่น ข้อความ รูปภาพ เสียง วิดิทัศน์ เป็นต้น

3. มาตรฐานการจัดชั้นความลับ (Data Classification Standard)

ส่วนงานเจ้าของข้อมูลมีหน้าที่แบ่งระดับชั้นความลับของข้อมูล อ้างอิงตามคำสั่งบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ที่ รบ.20/2564 เรื่อง การรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ ที่ระบุใน ST-04 มาตรฐานเรื่อง การบริหารจัดการทรัพย์สินของบริษัท โดยการกำหนดระดับความลับให้พิจารณาดังต่อไปนี้

ระดับความลับ	คำจำกัดความ	ตัวอย่าง
เปิดเผย (Public)	สารสนเทศที่เปิดเผยสู่สาธารณะ	- สารสนเทศที่เปิดเผยสู่ สาธารณะ - เอกสารเผยแพร่ ประชาสัมพันธ์ของบริษัท - ข้อมูลเกี่ยวกับสินค้าและบริการของบริษัท - รายงานประจำปีบริษัท - ประกาศการจัดซื้อจัดจ้าง
ข้อมูลใช้ภายในเท่านั้น (Internal Use only)	สารสนเทศที่ใช้เฉพาะภายในบริษัทเท่านั้น	- ระเบียบ คำสั่ง ของบริษัท - ข้อตกลงระดับการให้บริการ - ข้อมูลโครงสร้างองค์กร - เอกสารประกอบการดำเนินงานของบริษัท เช่น บันทึก รายงาน - ข้อมูลพนักงานสำหรับการติดต่อภายในบริษัท - ข้อมูลส่วนบุคคลเกี่ยวกับลูกค้า/คู่ค้า สำหรับการติดต่อภายในบริษัท
ลับ (Confidential)	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยต่อผู้ไม่มีอำนาจหน้าที่ในการรับทราบไม่ว่าทั้งหมดหรือเพียงบางส่วนจะเกิดความเสียหายแก่ประโยชน์ของบริษัท และ/หรือประโยชน์แห่งรัฐ	- ข้อมูลพนักงานสำหรับการติดต่อส่วนบุคคล - ข้อมูลส่วนบุคคลเกี่ยวกับการจ้างงาน - ข้อมูลส่วนบุคคลที่เกี่ยวกับครอบครัว - ข้อมูลส่วนบุคคลที่เกี่ยวกับการเงิน - ข้อมูล/เอกสารแผนงานที่มีการระบุงบประมาณ

ระดับความลับ	คำจำกัดความ	ตัวอย่าง
		- เอกสารข้อกำหนดที่ยังไม่ดำเนินการจัดหา - รายงานผลการตรวจสอบ - ข้อมูลส่วนบุคคลเกี่ยวกับลูกค้า/คู่ค้า
ลับมาก (Secret)	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยต่อผู้ไม่มีอำนาจหน้าที่ในการรับทราบไม่ว่าทั้งหมดหรือเพียงบางส่วนจะเกิดความเสียหายแก่ประโยชน์ของบริษัทและหรือประโยชน์แห่งรัฐอย่างร้ายแรง	
ลับที่สุด (Top Secret)	ข้อมูลข่าวสารลับซึ่งหากเปิดเผยต่อผู้ไม่มีอำนาจหน้าที่ในการรับทราบไม่ว่าทั้งหมดหรือเพียงบางส่วนจะเกิดความเสียหายแก่ประโยชน์ของบริษัท และหรือประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด	

การจัดเก็บและการสำรองข้อมูล

3.1 ผู้บริหารและผู้รับผิดชอบดูแลข้อมูลสารสนเทศเป็นผู้กำหนดระยะเวลาในการจัดเก็บข้อมูลสารสนเทศตามระดับความลับ

3.2 ข้อมูลที่เป็นความลับ หรือมีความสำคัญสูง ให้ทำการจัดเก็บแยกไว้ต่างหาก และป้องกันให้มีความปลอดภัยอย่างเพียงพอต่อการเข้าถึง เช่น การทำสัญลักษณ์ลายน้ำ และแสดงขั้นความลับกำกับทุกหน้าของไฟล์ เป็นต้น

3.3 การทำสำเนาข้อมูลที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูง ต้องได้รับอนุญาตจากเจ้าของข้อมูล

3.4 ผู้ปฏิบัติงานต้องทำการป้องกันข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยใช้รหัสผ่านที่มีความมั่นคงปลอดภัย

3.5 ผู้ปฏิบัติงานทำการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอ หรือตามที่คณะกรรมการกำกับดูแลข้อมูลกำหนด

3.6 รายงานคณะกรรมการด้านการพัฒนาเทคโนโลยีดิจิทัล (ตามคำสั่งคณะกรรมการบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ที่ 21/2564) ทันที เมื่อข้อมูลสารสนเทศหรืออุปกรณ์ซึ่งบรรจุข้อมูลสารสนเทศสูญหายหรือถูกขโมย

4. ความมั่นคงปลอดภัยของข้อมูล (Data Security)

4.1 การรักษาความลับ (Confidentiality) หมายถึง การรักษาข้อมูลตามสภาพของการจัดชั้นความลับ และมีการกำหนดสิทธิ์การเข้าถึงข้อมูลนั้น เนื่องจากข้อมูลในหน่วยงานอาจมีหลายประเภท ข้อมูลบางประเภทเป็นข้อมูลที่มีความสำคัญ หรืออ่อนไหว จึงต้องมีการรักษาความลับเพื่อลดความเสี่ยงของการถูกคุกคามและเป็นการป้องกันการรั่วไหลของข้อมูลโดยมิชอบ เช่น การส่งข้อมูลที่ปกปิดหรือเป็นความลับต้องมีวิธีการที่ทำให้ทราบได้ว่าบุคคลที่ต้องการส่งข้อมูลมาให้ หรือการที่ผู้ได้รับการอนุญาตให้เข้าถึงข้อมูลเท่านั้นที่สามารถอ่านข้อมูลได้

4.2 ความถูกต้องของข้อมูล (Integrity) หมายถึง การคงสภาพของข้อมูลหรือการรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความถูกต้องและน่าเชื่อถือ รวมถึงมีการปกป้องข้อมูลให้ปราศจากการถูกเปลี่ยนแปลงโดยผู้ไม่มีสิทธิ์ เช่น ข้อมูลที่ใช้จะต้องเป็นข้อมูลที่ถูกต้องอย่างแท้จริง ไม่มีการดัดแปลงหรือแก้ไขระหว่างทาง

4.3 ความพร้อมใช้งานของข้อมูล (Availability) หมายถึง การพร้อมในการใช้งานอยู่เสมอ กล่าวคือ ข้อมูลต้องพร้อมสำหรับการใช้งานได้เสมอ รวมถึงมีการสำรองข้อมูลไว้เมื่อเกิดภัยพิบัติหรือเหตุการณ์ที่ไม่คาดฝัน เช่น หากต้องการใช้ข้อมูล ผู้ใช้งานสามารถใช้ข้อมูลได้ทันที และใช้ได้อย่างต่อเนื่อง

5. การเปิดเผยข้อมูล (Open Data)

5.1 การเผยแพร่ข้อมูลข่าวสารใด ต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อน

5.2 เจ้าของข้อมูลต้องตรวจสอบความถูกต้องของข้อมูลก่อนอนุญาตนำออกเผยแพร่

5.3 ผู้ปฏิบัติงานห้ามเปิดเผยข้อมูลลับซึ่งได้มาจากการปฏิบัติงาน ทั้งที่เป็นข้อมูลของบริษัท หรือบุคคลภายนอก

6. คุณภาพของข้อมูล (Data Quality)

เป็นเครื่องมือในการวัดความน่าเชื่อถือและประสิทธิภาพของการนำข้อมูลไปใช้ต้องมีการวางแผนการดำเนินการ และการควบคุมกิจกรรมต่าง ๆ รวมถึงการปรับปรุง เพื่อให้ ข้อมูลมีคุณภาพ เนื่องจากข้อมูลที่มีคุณภาพสูงทำให้การดำเนินงานของหน่วยงานเป็นไปอย่างมีประสิทธิภาพ การทำให้ข้อมูลมีคุณภาพประกอบด้วย

6.1 การทำให้ข้อมูลมีความถูกต้อง (Accuracy)

6.2 ข้อมูลมีความครบถ้วน (Completeness)

6.3 ข้อมูลมีความต้องกัน (Consistency)

6.4 ข้อมูลมีความเป็นปัจจุบัน (Timeliness)

6.5 ข้อมูลตรงตามความต้องการของผู้ใช้ (Relevancy)

6.6 ข้อมูลมีความพร้อมใช้ (Availability)

วิธีการดำเนินการ	• กำหนดข้อมูลที่จำเป็นต้องมีคุณภาพ • พัฒนาและส่งเสริมการให้ความสำคัญกับคุณภาพของข้อมูล (Awareness) • กำหนดขอบเขตของการประเมิน (Assessment) คุณภาพของข้อมูล • กำหนดและระบุลำดับความสำคัญ (Prioritize) ของการปรับปรุงข้อมูลให้มีคุณภาพ
สิ่งที่นำเข้า	• มาตรฐาน แนวปฏิบัติ และนโยบายที่เกี่ยวกับการทำให้ข้อมูลมีคุณภาพ เช่น การจัดทำโปรไฟล์ข้อมูล (Data Profiling) การทำความสะอาดข้อมูล (Data Cleansing) • เมทาดาตาทั้งด้านธุรกิจและเทคโนโลยีสารสนเทศ
เครื่องมือที่ใช้	• เครื่องมือในการทำความสะอาดข้อมูล (Data Cleansing Tools) • เครื่องมือวิเคราะห์ทางสถิติ (Statistical Analysis Tools)
ผลที่ได้รับ	• รายงานการรับรองคุณภาพของข้อมูล (Data Quality Certification Reports) • ข้อตกลงระดับคุณภาพของข้อมูล (Data Quality Service Level Agreements)
ผู้เกี่ยวข้อง	• นักวิเคราะห์ข้อมูล (Data Analyst) • บริกรข้อมูล (Data Stewards)

7. การทำลายข้อมูล

ให้ผู้ปฏิบัติงานปฏิบัติตามแนวทางการทำลายข้อมูลลับประเภทต่าง ๆ ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการนำสื่อบันทึกกลับมาใช้ใหม่	วิธีการทำลาย
CD/DVD		ใช้การทุบ หรือทำลายให้เสียหาย
สื่อบันทึกข้อมูลแบบถอด แยกได้ เช่น Flash Drive	ใช้การ Format	ใช้การทุบ หรือทำลายให้เสียหาย
ฮาร์ดดิสก์	ใช้การ Format โดยแบ่งตามระดับชั้นความลับ ดังนี้ - ใช้วิธีเขียนทับซ้ำจำนวน 1 ครั้ง ตามมาตรฐาน NIST 800-88 สำหรับข้อมูลที่เป็นชั้นความลับทั่วไปหรือลับ - ใช้วิธีเขียนทับซ้ำจำนวน 3 ครั้ง ตามมาตรฐาน DoD 5220.222-M สำหรับข้อมูลที่มีชั้นความลับระดับลับมาก - ใช้วิธีเขียนทับซ้ำจำนวน 7 ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลที่มีชั้นความลับระดับลับที่สุด	ใช้การทุบ หรือทำลายให้เสียหาย
กระดาษ	ขีดข้อความทิ้งก่อนนำไปใช้เป็นกระดาษ Reuse สำหรับเอกสารที่เป็นชั้นความลับระดับทั่วไป	ใช้เครื่องทำลายเอกสารก่อนทิ้งสำหรับเอกสารที่เป็นชั้นความลับทุกระดับ

8. การบริหารการแลกเปลี่ยนข้อมูลกับบุคคลภายนอก

8.1 กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจน ตั้งแต่ก่อนดำเนินการ เริ่มดำเนินการ ระหว่างดำเนินการ และ สิ้นสุดดำเนินการ

8.2 ทำงานร่วมกับทีมบริกรข้อมูล เพื่อจัดทำเมทาดาตา (Metadata) ของชุดข้อมูลให้ครบถ้วน และกำหนดเทคโนโลยี รวมถึงมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

8.3 จัดทำสัญญาหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูล และการนำข้อมูลไปใช้ ตรวจสอบการแลกเปลี่ยนข้อมูลให้เป็นไปตามแนวทาง มาตรฐาน และ สัญญาหรือข้อตกลงที่กำหนด

9. โครงสร้างการกำกับดูแลข้อมูล

นโยบายฉบับนี้ครอบคลุมข้อมูลทั้งที่อยู่ในและนอกระบบคอมพิวเตอร์ของบริษัท ทั้งที่อยู่ภายในและภายนอกสถานที่ปฏิบัติงานของบริษัท รวมทั้งคลาวด์ (Cloud) ที่บริษัทใช้จัดเก็บข้อมูลด้วย ซึ่งครอบคลุมถึงบุคคลดังต่อไปนี้

1) คณะกรรมการกำกับดูแลข้อมูล

2) ทีมบริกรข้อมูล

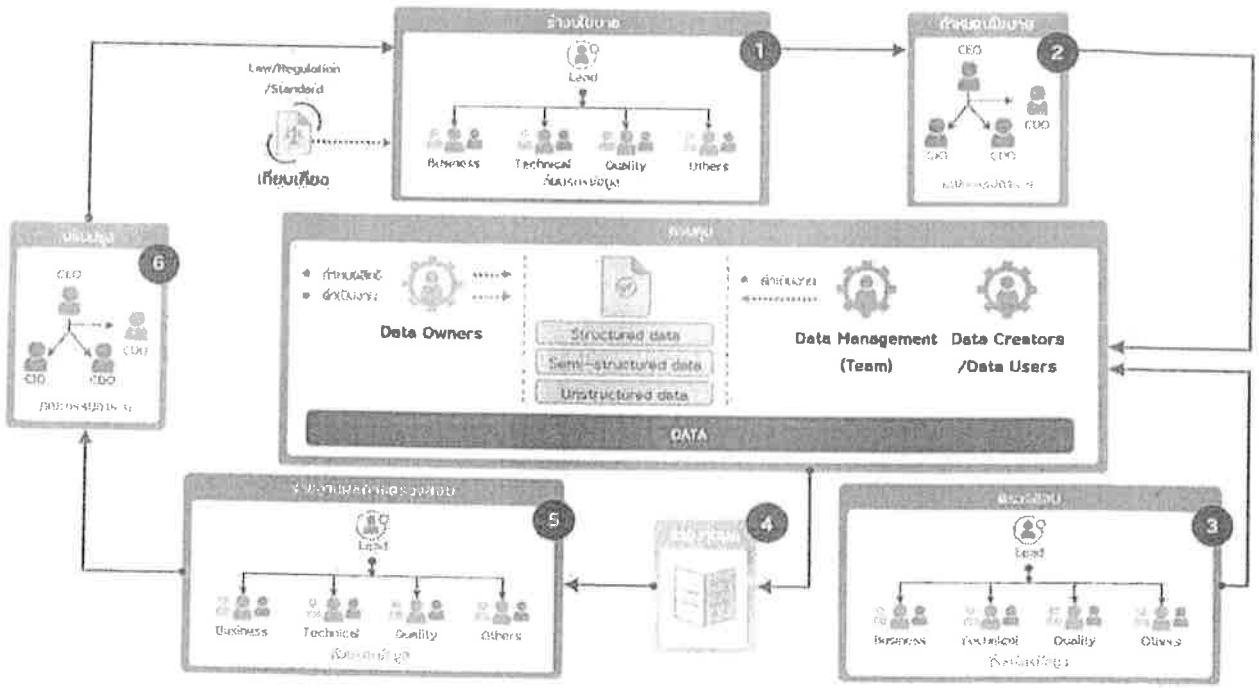
3) ทีมบริหารจัดการข้อมูล

4) เจ้าของข้อมูล

5) ผู้สร้างข้อมูล

6) ผู้ใช้ข้อมูล

7) ผู้ปฏิบัติงาน และบุคคลภายนอก



เป้าหมาย : เพื่อให้การบริหารจัดการข้อมูลเป็นไปอย่างถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย รักษาความเป็นบุคคล และป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูล

10. บทบาทหน้าที่และความรับผิดชอบ

10.1 คณะกรรมการกำกับดูแลข้อมูล

10.1.1 ทำหน้าที่ในการกำหนดเป้าหมายในการกำกับดูแลข้อมูล เพื่อให้สอดคล้องกับแผน กลยุทธ์ขององค์กร และเป็นแนวทางให้กับทีมบริหารจัดการข้อมูล เป็นผู้กำหนด (จัดทำ) นโยบาย มาตรฐาน กฎ ระเบียบ คู่มือ และแนวทางปฏิบัติ บทบาทหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องกับการกำกับดูแลข้อมูล และให้การสนับสนุนการปฏิบัติงานของบริษัทเป็นไปตามนโยบายการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่

10.1.2 กำกับดูแล และติดตามการดำเนินงานที่เกี่ยวข้องกับข้อมูล รวมถึงให้คำปรึกษาและตัดสินประเด็นสำคัญที่เกี่ยวข้องกับข้อมูล การรักษาข้อมูลในระบบและนอกระบบของส่วนงานให้เป็นไปตามนโยบายและมาตรฐานตามการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่

10.1.3 ดูแลให้มีการจัดทำ ทบทวน และปรับปรุงนโยบาย การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่

10.1.4 สนับสนุน ส่งเสริม และผลักดันการกำกับดูแลข้อมูล อย่างทั่วถึงและต่อเนื่อง

10.1.5 ดูแลและสนับสนุนให้มีการสื่อสารกับบุคลากรในองค์กรให้ตระหนักถึงความสำคัญของข้อมูล การใช้ข้อมูลอย่างปลอดภัย เพื่อให้เกิดการกำกับดูแลข้อมูลที่ดีภายในสถาบันการเงิน

10.1.6 พิจารณาบทลงโทษแก่ผู้กระทำความผิดตามนโยบายการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่

10.2 ทีมบริกรข้อมูล

10.2.1 ออกแบบกระบวนการจัดทำมาตรฐานเมทาดาตา (Metadata)

10.2.2 ออกแบบเกณฑ์ในการประเมินคุณภาพข้อมูลหน่วยงานให้เป็นไปตามเกณฑ์ด้านคุณภาพข้อมูลมาตรฐานสากล ได้แก่ ความถูกต้อง (Accuracy) ความสมบูรณ์ของข้อมูล (Completeness) ความตรงกัน (Consistency) มีความเป็นปัจจุบัน (Timeliness) ตรงความต้องการของผู้ใช้ (Relevancy) ความน่าเชื่อถือได้ของข้อมูล (Credibility) และมีความพร้อมใช้งาน (Availability)

10.2.3 ร่างแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับข้อมูลเพื่อให้เกิดความเข้าใจถูกต้องตรงกันภายในบริษัท

10.2.4 วิเคราะห์ ตรวจสอบ แก้ไขปัญหา และสรุปผลการดำเนินงานในแต่ละด้านพร้อมกับข้อเสนอแนะ เพื่อเป็นข้อมูลให้แก่ทีมบริหารจัดการข้อมูลเพื่อดำเนินการต่อไป

10.3 ทีมบริหารจัดการข้อมูล

10.3.1 พัฒนาสถาปัตยกรรม กำหนดโครงสร้าง และความสัมพันธ์ของข้อมูล

10.3.2 จัดทำดัชนีข้อมูลและรูปแบบการจัดเก็บ เรียกใช้ และสำรองข้อมูล

10.3.3 วิเคราะห์ข้อมูล หรือแก้ไขปัญหา โดยใช้หลักทางสถิติ

10.3.4 รวบรวมข้อมูลจากหลายๆ แหล่ง และแปลงข้อมูล เพื่อหารูปแบบและความสัมพันธ์ของข้อมูล

10.3.5 ตรวจสอบการปฏิบัติตามนโยบาย มาตรฐาน กฎ ระเบียบ คู่มือ และแนวทางปฏิบัติของคณะกรรมการกำกับดูแลข้อมูล

10.3.6 ให้คำปรึกษาในการจัดทำเมตาดาตา (Metadata) ร่างนโยบายข้อมูลและมาตรฐานที่เกี่ยวข้องกับข้อมูล

10.4 เจ้าของข้อมูล

10.4.1 ทบทวน และการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล เช่น การปรับปรุงเมตาดาตา (Metadata) และเกณฑ์การทำความสะอาดข้อมูล (Data Cleansing) เป็นต้น

10.4.2 กำหนดสิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

10.4.3 สนับสนุนทีมบริกรข้อมูล และทีมบริหารจัดการข้อมูลในการจัดทำมาตรฐาน และนโยบายที่เกี่ยวข้องกับข้อมูล

10.5 ผู้สร้างข้อมูล

10.5.1 บันทึก แก้ไข ปรับปรุง หรือลบข้อมูล ตามนโยบาย มาตรฐาน กฎ ระเบียบ คู่มือ และแนวทางปฏิบัติที่เกี่ยวข้อง

10.5.2 สนับสนุนทีมบริกรข้อมูลตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความมั่นคงปลอดภัย

10.6 ผู้ใช้ข้อมูล

10.6.1 ปฏิบัติตามนโยบาย มาตรฐาน และระเบียบวิธีปฏิบัติที่เกี่ยวข้องกับการกำกับดูแลข้อมูล

10.6.2 สนับสนุนการกำกับดูแลข้อมูลให้ความต้องการในการใช้ข้อมูล

10.6.3 รายงานปัญหาที่พบระหว่างการใช้ข้อมูล ทั้งด้านคุณภาพและความปลอดภัยของข้อมูล ให้กับทีมบริกรข้อมูล

10.7 ผู้ปฏิบัติงาน และบุคคลภายนอก

10.7.1 รับทราบและถือปฏิบัติตามนโยบาย มาตรฐาน กฎ ระเบียบ คู่มือ และแนวทางปฏิบัติของบริษัทที่เกี่ยวข้องในการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่โดยเคร่งครัด

10.7.2 ให้ความร่วมมือในการป้องกันข้อมูลของบริษัท และแจ้งให้ผู้บังคับบัญชาทราบทันทีเมื่อพบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสมที่อาจสร้างความเสียหายกับข้อมูลของบริษัท

11. การทบทวนนโยบายและแนวปฏิบัติ

บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) จัดให้มีการติดตาม และรายงานผลต่อผู้บริหารระดับสูง คณะกรรมการด้านการพัฒนาเทคโนโลยีดิจิทัลอย่างสม่ำเสมอ และมีการทบทวนนโยบายฉบับนี้อย่างน้อยปีละ 1 ครั้ง เพื่อให้การดำเนินงานเป็นไปตามนโยบายการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ที่กำหนด