นโยบายการกำกับดูแลและบริหารจัดการข้อมูล
บริษัท บริการเชื้อเพลิงการบินกรุงเทพ จำกัด (มหาชน)

จัดทำครั้งที่	1.0
วันที่มีผลบังคับใช้	วันที่ 11 พฤศจิกายน 2569
อนุมัติโดย	มติคณะกรรมการบริษัท ในการประชุมครั้งที่ 4/2569 วันที่ 11 พฤศจิกายน 2569
	ม.ร.ว.ศุภดิศ ดิศกุล ประธานกรรมการบริษัท

นโยบายการกำกับดูแลและบริหารจัดการข้อมูล
(Data Governance Policy)

1. หลักการ

บริษัท บริการเชื้อเพลิงการบินกรุงเทพ จำกัด (มหาชน) (“บริษัท”) และบริษัทย่อย ตระหนักว่าข้อมูลเป็นทรัพยากรสำคัญของบริษัท ซึ่งมีบทบาทสำคัญต่อการดำเนินธุรกิจ การกำหนดกลยุทธ์ การตัดสินใจ การบริหารความเสี่ยง การพัฒนานวัตกรรม ตลอดจนการปฏิบัติตามกฎหมาย ระเบียบ ข้อกำหนด และมาตรฐานที่เกี่ยวข้อง ดังนั้น บริษัทจึงกำหนดให้มีการกำกับดูแลข้อมูล (Data Governance) เพื่อให้ข้อมูลขององค์กรได้รับการบริหารจัดการอย่างเป็นระบบ มีคุณภาพ ถูกต้อง ครบถ้วน เป็นปัจจุบัน ปลอดภัย และสามารถนำไปใช้ได้อย่างมีประสิทธิภาพตลอดวงจรชีวิตของข้อมูล (Data Lifecycle)

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดหลักเกณฑ์ วิธีปฏิบัติ บทบาทหน้าที่ และแนวทางควบคุมที่เกี่ยวข้องกับข้อมูลให้เป็นมาตรฐานเดียวกันทั่วทั้งบริษัท เพื่อให้ผู้บริหาร พนักงาน และผู้ที่เกี่ยวข้องใช้เป็นแนวทางในการปฏิบัติงานอย่างถูกต้อง สอดคล้องกับหลักธรรมาภิบาลขององค์กร สนับสนุนการใช้ข้อมูลอย่างมีประสิทธิภาพ ลดความเสี่ยงที่อาจเกิดขึ้นจากการบริหารจัดการข้อมูล และสร้างความเชื่อมั่นให้แก่ผู้มีส่วนได้เสียทุกภาคส่วน

2. วัตถุประสงค์

1. เพื่อใช้เป็นแนวทางปฏิบัติในการกำกับดูแลและบริหารจัดการข้อมูลของบริษัทให้เป็นมาตรฐานเดียวกัน
2. เพื่อกำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องกับข้อมูลอย่างชัดเจน
3. เพื่อกำหนดแนวทางการพัฒนาคุณภาพข้อมูลของบริษัท
4. เพื่อกำหนดแนวทางในการใช้และการรักษาความมั่นคงปลอดภัยของข้อมูลอย่างเหมาะสม
5. เพื่อให้หน่วยงานสามารถดำเนินการเกี่ยวกับข้อมูลได้อย่างถูกต้อง สอดคล้องกับกฎหมาย ระเบียบ และข้อกำหนดที่เกี่ยวข้อง
6. เพื่อสนับสนุนการนำข้อมูลไปใช้ประโยชน์ในการดำเนินงานและการตัดสินใจอย่างมีประสิทธิภาพ

3. ขอบเขตการบังคับใช้

นโยบายฉบับนี้ให้ใช้บังคับกับข้อมูลทั้งหมดของบริษัท ไม่ว่าจะอยู่ในรูปแบบเอกสาร ระบบสารสนเทศ ฐานข้อมูล หรือข้อมูลอิเล็กทรอนิกส์อื่นใด รวมถึงบุคลากร คู่ค้า ผู้รับจ้าง และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึง ใช้ เปิดเผย จัดเก็บ หรือบริหารจัดการข้อมูลของบริษัท

4. คำนิยาม

- ข้อมูล (Data) หมายถึง ข้อเท็จจริงหรือสารสนเทศที่สื่อความหมาย ไม่ว่าจะโดยผ่านวิธีการใด ๆ หรือจะได้จัดทำไว้ในรูปแบบใด อาทิ ในรูปแบบเอกสาร แฟ้ม รายงาน ภาพถ่าย การบันทึกภาพหรือเสียง การบันทึกโดยคอมพิวเตอร์ หรือ วิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏและสามารถนำไปใช้ประโยชน์ในการดำเนินงานได้
- ข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
- ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) หมายถึง ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดในทำนองเดียวกันตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด ซึ่งต้องมีฐานทางกฎหมายและมาตรการคุ้มครองที่เข้มงวดกว่าข้อมูลส่วนบุคคลทั่วไป
- การละเมิดข้อมูลส่วนบุคคล (Personal Data Breach) หมายถึง การละเมิดมาตรการรักษาความมั่นคงปลอดภัยที่เป็นเหตุให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยไม่ชอบด้วยกฎหมาย ไม่ว่าจะเกิดจากเจตนา ความประมาท อุบัติเหตุ หรือสาเหตุอื่นใด
- คณะทำงานธรรมาภิบาลข้อมูล (Data Governance Working Group: DWG) หมายถึง คณะทำงานที่ได้รับแต่งตั้งตามคำสั่งของบริษัทให้รับผิดชอบและกำกับดูแลการบริหารจัดการข้อมูลของบริษัท
- ชุดข้อมูล (Dataset) หมายถึง การรวบรวมข้อมูลที่มีความสัมพันธ์กันและจัดทำขึ้นเพื่อใช้ประโยชน์ตามวัตถุประสงค์ที่กำหนด
- ทะเบียนข้อมูล (Data Inventory) หมายถึง เอกสารหรือระบบที่ใช้บันทึกสินทรัพย์ข้อมูล แหล่งจัดเก็บข้อมูล และระบบสารสนเทศของบริษัท โดยระบุรายละเอียดที่สำคัญ เช่น หน่วยงานเจ้าของข้อมูล ประเภทข้อมูล ระดับชั้นข้อมูล สถานที่จัดเก็บ วัตถุประสงค์การใช้งาน ระยะเวลาการเก็บรักษา และวิธีการทำลายหรือกำจัดข้อมูล เพื่อสนับสนุนการกำกับดูแลข้อมูลและการปฏิบัติตามข้อกำหนดทางกฎหมาย
- บัญชีข้อมูล (Data Catalog) หมายถึง เอกสารหรือระบบที่ใช้รวบรวม จัดหมวดหมู่ และแสดงรายการชุดข้อมูลของบริษัท พร้อมข้อมูลกำกับ (Metadata) ที่สำคัญ เช่น คำอธิบายชุดข้อมูล หน่วยงานเจ้าของข้อมูล แหล่งที่มาของข้อมูล รูปแบบข้อมูล ความถี่ในการปรับปรุงข้อมูล และเงื่อนไขหรือสิทธิการใช้งานข้อมูล เพื่อให้ผู้ใช้งานสามารถค้นหา ทำความเข้าใจ และใช้ประโยชน์จากข้อมูลได้อย่างถูกต้องและมีประสิทธิภาพ
- เมทาดาตา (Metadata) หมายถึง คำอธิบายข้อมูลที่แสดงรายละเอียดเกี่ยวกับโครงสร้าง ความหมาย แหล่งที่มา และสิทธิในการเข้าถึงข้อมูล

- เจ้าของข้อมูล (Data Owner) หมายถึง หน่วยงานหรือบุคคลที่มีหน้าที่รับผิดชอบข้อมูลชุดนั้นโดยตรง ไม่ว่าจะเป็นกรณีที่ได้จัดทำข้อมูลนั้นขึ้นมาใหม่ หรือรับข้อมูลจากบุคคลอื่น
- ผู้ดูแลข้อมูล (Data Steward) หมายถึง ผู้ที่ได้รับมอบหมายให้กำกับดูแลและบริหารจัดการข้อมูลในเชิงปฏิบัติของแต่ละฝ่าย และ/หรือ สำนัก
- ผู้สร้างข้อมูล (Data Creator) หมายถึง ผู้ที่มีหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้เป็นไปตามมาตรฐานที่กำหนด
- ผู้ใช้ข้อมูล (Data User) หมายถึง ผู้ที่ได้รับอนุญาตให้เข้าถึงหรือใช้ข้อมูลตามสิทธิและหน้าที่ที่กำหนด
- ผู้ดูแลระบบสารสนเทศ (System Administrator) หมายถึง ผู้ที่รับผิดชอบดูแลระบบสารสนเทศ ระบบฐานข้อมูล และโครงสร้างพื้นฐานด้านเทคโนโลยีที่เกี่ยวข้องกับข้อมูล
- หน่วยงาน หมายถึง ฝ่าย สำนัก หรือคณะทำงานภายในบริษัท ซึ่งมีหน้าที่หรือความรับผิดชอบเกี่ยวกับการจัดทำ จัดเก็บ รวบรวม ใช้ เปิดเผย เผยแพร่ หรือดำเนินการอื่นใดที่เกี่ยวข้องกับข้อมูลของบริษัท ไม่ว่าทั้งหมดหรือบางส่วน ทั้งนี้ ตามขอบเขตอำนาจหน้าที่และความรับผิดชอบของแต่ละหน่วยงาน

5. โครงสร้างการกำกับดูแลข้อมูล

5.1 คณะทำงานธรรมาภิบาลข้อมูล

ให้มีหน้าที่กำหนดนโยบาย เป้าหมาย และแนวทางการบริหารจัดการข้อมูลของบริษัท กำกับติดตามผลการดำเนินงานและให้ความเห็นชอบมาตรฐานข้อมูลที่สำคัญ ตลอดจนกำกับทิศทางการบริหารจัดการข้อมูลของบริษัทในภาพรวม กำหนดยุทธศาสตร์และเป้าหมาย รวมทั้งผลักดันการดำเนินงานด้านธรรมาภิบาลข้อมูลให้เป็นไปตามนโยบายฉบับนี้

5.2 เจ้าของข้อมูล (Data Owner)

ให้มีหน้าที่กำหนดแนวทางที่เกี่ยวข้องกับคำอธิบายข้อมูล การจัดทำทะเบียนข้อมูล การกำหนดระดับชั้นข้อมูล การกำหนดแนวทางในการดูแลรักษาคุณภาพของข้อมูล กำหนดสิทธิการเข้าถึงข้อมูลนั้น ๆ และอนุมัติการใช้ข้อมูลตามความเหมาะสม หากมีการขอใช้ข้อมูล เจ้าของข้อมูลควรมีการทบทวนว่าข้อมูลนั้น ๆ สามารถใช้ฐานเดิมในการเก็บและประมวลผลได้อยู่หรือไม่ รวมทั้งจัดให้มีและปรับปรุงบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (Records of Processing Activities: ROPA) สำหรับข้อมูลส่วนบุคคลภายใต้ความรับผิดชอบของตนให้เป็นปัจจุบัน เพื่อใช้เป็นข้อมูลนำเข้าสำหรับทะเบียนข้อมูลและบัญชีข้อมูลตามข้อ 9

5.3 ผู้ดูแลข้อมูล (Data Steward)

ให้มีหน้าที่ดำเนินการด้านข้อมูลในเชิงปฏิบัติ จัดทำและปรับปรุงเมทาดาตา ติดตามคุณภาพข้อมูล และประสานงานกับหน่วยงานที่เกี่ยวข้อง

5.4 ผู้สร้างข้อมูล (Data Creator)

ให้มีหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลตามมาตรฐานที่กำหนด และรายงานปัญหาด้านคุณภาพข้อมูลหรือความมั่นคงปลอดภัยให้ผู้เกี่ยวข้องทราบโดยไม่ชักช้า

5.5 ผู้ดูแลระบบสารสนเทศ (System Administrator)

ให้มีหน้าที่ดูแลระบบสารสนเทศ ระบบฐานข้อมูล และโครงสร้างพื้นฐานด้านเทคโนโลยีที่เกี่ยวข้องกับข้อมูล รวมทั้งดำเนินการด้านความมั่นคงปลอดภัย การสำรองข้อมูล และการกู้คืนข้อมูลตามมาตรการที่บริษัทกำหนด

5.6 ผู้ใช้ข้อมูล (Data User)

ให้ใช้หรือเปิดเผยข้อมูลของบริษัท เฉพาะตามวัตถุประสงค์และเงื่อนไขที่ได้รับอนุญาตเท่านั้น รวมทั้ง มีหน้าที่ต้องปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัยและข้อกำหนดของบริษัทอย่างเคร่งครัด

5.7 แผนกกฎหมาย

ให้มีหน้าที่ให้คำแนะนำเกี่ยวกับระยะเวลาการเก็บรักษาข้อมูลตามกฎหมายและตามสัญญา ออกและยกเลิกคำสั่งระงับการทำลาย (Legal Hold) และจัดทำรายการคำสั่งระงับการทำลายที่ยังมีผลใช้บังคับ

5.8 คณะทำงานคุ้มครองข้อมูลส่วนบุคคล

ให้มีหน้าที่กำกับดูแลการบริหารจัดการข้อมูลส่วนบุคคลตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลและแนวปฏิบัติที่เกี่ยวข้อง

5.9 ฝ่ายตรวจสอบภายใน

ให้มีหน้าที่ตรวจสอบการปฏิบัติตามนโยบายฉบับนี้และแนวปฏิบัติที่ออกตามนโยบายนี้ตามรอบที่วางแผนไว้ และรายงานข้อบกพร่องที่พบ

6. ด้านคุณภาพข้อมูล

ให้เจ้าของข้อมูลและหน่วยงานที่เกี่ยวข้องดำเนินการวัดและประเมินคุณภาพข้อมูลอย่างต่อเนื่อง โดยพิจารณาอย่างน้อย 5 มิติ ดังต่อไปนี้

- ความถูกต้องและความครบถ้วน (Accuracy and Completeness) หมายถึง ข้อมูลมีความถูกต้องแม่นยำ และครบถ้วนสมบูรณ์ พร้อมผ่านการตรวจสอบในทุกขั้นตอน เพื่อให้สามารถนำไปใช้ได้อย่างน่าเชื่อถือ
- ความสอดคล้องกัน (Consistency) หมายถึง ข้อมูลมีความสอดคล้องกันในด้านแนวคิด คำนิยาม วิธีการ รหัส และรูปแบบการนำเสนอ เพื่อให้สามารถเปรียบเทียบและบูรณาการข้อมูลจากต่างแหล่งหรือต่างช่วงเวลาได้

- ความเป็นปัจจุบัน (Timeliness) หมายถึง ข้อมูลได้รับการปรับปรุงให้ทันต่อเหตุการณ์และพร้อมใช้งานภายในระยะเวลาที่เหมาะสมตามวัตถุประสงค์การใช้งาน
- ความสอดคล้องกับความต้องการใช้งาน (Relevancy) หมายถึง ข้อมูลมีความเหมาะสม สอดคล้องกับวัตถุประสงค์ของงาน และมีระดับรายละเอียดเพียงพอต่อการนำไปใช้
- ความพร้อมใช้งาน (Availability) หมายถึง ข้อมูลสามารถเข้าถึงและใช้งานได้ตามสิทธิ์ ภายใต้เงื่อนไขและช่วงเวลาที่กำหนด

7. การจัดชั้นข้อมูล

การจำแนกระดับชั้นข้อมูลให้พิจารณาตามระดับความสำคัญและผลกระทบที่อาจเกิดขึ้นจากการเปิดเผย การสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อกำหนดมาตรการควบคุมการเข้าถึงและการคุ้มครองข้อมูลให้เหมาะสม โดยแบ่งระดับชั้นข้อมูลเป็น 4 ระดับ ได้แก่ ข้อมูลสาธารณะ (Public) ข้อมูลใช้ภายในบริษัท (Internal Use) ข้อมูลลับ (Confidential) และข้อมูลลับมาก (Restricted) ทั้งนี้ หลักเกณฑ์ วิธีการ ขั้นตอน และอำนาจในการพิจารณาอนุมัติการจำแนกระดับชั้นข้อมูล ให้เป็นไปตามที่กำหนดไว้ในแนวปฏิบัติการจำแนกประเภทและการจัดการข้อมูลของบริษัท รวมถึงที่อาจมีการแก้ไขเพิ่มเติมหรือใช้บังคับแทนในภายหน้า

8. ความมั่นคงปลอดภัยและการคุ้มครองข้อมูล

ให้เจ้าของข้อมูล และหน่วยงานที่เกี่ยวข้อง กำหนดและดำเนินมาตรการด้านความมั่นคงปลอดภัยสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคลให้สอดคล้องกับกฎหมาย มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง รวมถึงการควบคุมสิทธิการเข้าถึง การสำรองข้อมูล การกู้คืนข้อมูล และการติดตามการใช้งานข้อมูลโดยอย่างน้อยให้ครอบคลุมองค์ประกอบดังต่อไปนี้

- การตอบสนองต่อเหตุการณ์ผิดปกติและการละเมิดข้อมูล (Incident Response and Data Breach Notification): ให้มีขั้นตอนการตรวจพบ ประเมินความเสี่ยง รายงาน และแจ้งเหตุการละเมิดข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายในระยะเวลาที่กฎหมายกำหนด รวมถึงแจ้งเจ้าของข้อมูลส่วนบุคคลในกรณีที่การละเมิดมีความเสี่ยงสูงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล
- มาตรฐานการยืนยันตัวตนและรหัสผ่าน (Authentication Standards): ให้กำหนดมาตรฐานขั้นต่ำสำหรับการยืนยันตัวตนก่อนเข้าถึงระบบและข้อมูลของบริษัท โดยความเข้มงวดของมาตรการให้เป็นไปตามระดับชั้นของข้อมูลที่เข้าถึง
- การบริหารจัดการสิทธิการเข้าถึงระดับสูง (Privileged Access Management): ให้ควบคุม อนุมัติ และทบทวนสิทธิการเข้าถึงของผู้ดูแลระบบและผู้มีสิทธิการเข้าถึงระดับสูงเป็นการเฉพาะ แยกจากสิทธิของผู้ใช้งานทั่วไป และบันทึกการใช้งานสิทธิดังกล่าวเพื่อประโยชน์ในการตรวจสอบย้อนหลัง

- การเข้ารหัสข้อมูลตามระดับชั้นข้อมูล (Encryption by Classification Level): ให้กำหนดมาตรการเข้ารหัสข้อมูลทั้งในระหว่างการจัดเก็บและระหว่างการส่งผ่าน ตามความเหมาะสมกับระดับชั้นข้อมูลตามข้อ 7 โดยข้อมูลลับและข้อมูลลับมากต้องได้รับการเข้ารหัสเป็นอย่างน้อย
- การควบคุมการเข้าถึงข้อมูลของบุคคลภายนอก (Third-Party Access Control): ให้บุคคลภายนอก คู่ค้า หรือผู้รับจ้างที่ต้องเข้าถึงข้อมูลของบริษัท ปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไม่ต่ำกว่ามาตรฐานที่บริษัทกำหนด และต้องมีข้อตกลงเป็นลายลักษณ์อักษรกำหนดขอบเขต หน้าที่ และความรับผิดชอบด้านการคุ้มครองข้อมูลไว้อย่างชัดเจนก่อนการเข้าถึง

รายละเอียดวิธีปฏิบัติทางเทคนิคภายใต้แต่ละองค์ประกอบข้างต้น ให้เป็นไปตามมาตรฐานหรือคู่มือด้านความมั่นคงปลอดภัยสารสนเทศของบริษัท

9. การจัดทำบัญชีข้อมูลและเมทาดาตา (Data Catalog & Metadata)

ให้ทุกหน่วยงานในบริษัทจัดทำและปรับปรุงบัญชีข้อมูลและเมทาดาตาสำหรับข้อมูลสำคัญของบริษัท เพื่อให้สามารถค้นหา เชื่อมโยง ใช้งาน และบริหารจัดการข้อมูลได้อย่างมีประสิทธิภาพและตรวจสอบได้

- **ความหมายของบัญชีข้อมูล (Data Catalog)**
    - เป็นแหล่งรวบรวมรายการข้อมูลสำคัญของบริษัทในลักษณะศูนย์กลาง
    - ช่วยให้ผู้ใช้ข้อมูลสามารถค้นหา เข้าถึง และทำความเข้าใจข้อมูลได้อย่างสะดวกและถูกต้อง
    - ทำหน้าที่เสมือนสารบัญข้อมูลของบริษัท
- **ความหมายของเมทาดาตา (Metadata)**
    - เป็นข้อมูลที่ใช้อธิบายรายละเอียดของข้อมูล
    - ใช้แสดงบริบทของข้อมูล เช่น ความหมาย แหล่งที่มา รูปแบบ และวิธีการใช้งาน
    - ช่วยให้ข้อมูลสามารถตีความและนำไปใช้งานได้อย่างถูกต้องและเหมาะสม
- **วัตถุประสงค์ของการจัดทำ**
    - เพื่อให้สามารถค้นหาและเข้าถึงข้อมูลได้อย่างรวดเร็ว เป็นระบบ และตรวจสอบได้
    - เพื่อสนับสนุนการเชื่อมโยงข้อมูลจากหลายแหล่ง
    - เพื่อเสริมสร้างความน่าเชื่อถือและความเข้าใจที่ถูกต้องเกี่ยวกับข้อมูล
    - เพื่อสนับสนุนการกำกับดูแลข้อมูลและความมั่นคงปลอดภัยของข้อมูล
    - เพื่อส่งเสริมการใช้ข้อมูลร่วมกันภายในบริษัทอย่างเหมาะสม
- **องค์ประกอบของเมทาดาตาที่ควรมี**
    - ข้อมูลด้านเทคนิค (Technical Metadata) เช่น โครงสร้างข้อมูล รูปแบบไฟล์ และแหล่งจัดเก็บ
    - ข้อมูลด้านธุรกิจ (Business Metadata) เช่น คำอธิบายข้อมูล ความหมาย และเจ้าของข้อมูล
    - ข้อมูลด้านการดำเนินงาน (Operational Metadata) เช่น วันที่ปรับปรุง ความถี่การใช้งาน และประวัติการเข้าถึง

- **แนวทางการดำเนินการในบริษัท**
    - กำหนดมาตรฐานการจัดทำเมทาดาตาให้เป็นรูปแบบเดียวกัน
    - กำหนดเจ้าของข้อมูล (Data Owner) และผู้ดูแลข้อมูล (Data Steward) ให้ชัดเจน
    - กำหนดระดับชั้นข้อมูลและสิทธิการเข้าถึงให้เหมาะสม
    - บันทึกแหล่งที่มาและความเชื่อมโยงของข้อมูล (Data Lineage)
    - ทบทวนและปรับปรุงข้อมูลให้เป็นปัจจุบันอย่างสม่ำเสมอ
    - ใช้ทะเบียนข้อมูลซึ่งจัดทำตามแนวปฏิบัติว่าด้วยเรื่อง การเก็บ รักษา และทำลายข้อมูลทั่วไป และบันทึกรายการประมวลผลข้อมูลส่วนบุคคล (ROPA) เป็นข้อมูลตั้งต้นในการจัดทำบัญชีข้อมูล

10. การเชื่อมโยงและแลกเปลี่ยนข้อมูล

การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานภายในและภายนอกต้องดำเนินการตามมาตรฐาน กระบวนการ และข้อกำหนดด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง โดยต้องอ้างอิงเมทาดาตาและจัดเก็บบันทึกประวัติการรับ ส่ง และเชื่อมโยงข้อมูลเพื่อให้สามารถตรวจสอบย้อนหลังได้

11. วงจรชีวิตข้อมูล

- การสร้างข้อมูล (Create) ให้กำหนดมาตรฐานข้อมูล รูปแบบข้อมูล และผู้รับผิดชอบในการนำเข้าข้อมูลให้ชัดเจน
- การรวบรวมและจัดเก็บข้อมูล (Collect/Store) ให้ดำเนินการตามวัตถุประสงค์การใช้งาน พร้อมทั้งจัดให้มีมาตรการด้านความมั่นคงปลอดภัยและการสำรองข้อมูลอย่างเหมาะสม ทั้งนี้ ให้จัดเก็บข้อมูลเฉพาะในระบบหรือสถานที่ที่บริษัทกำหนด และลงทะเบียนระบบ ที่เก็บข้อมูล และสถานที่จัดเก็บไว้ในทะเบียนข้อมูล (Data Inventory) ตามแนวปฏิบัติว่าด้วยเรื่อง การเก็บ รักษา และทำลายข้อมูลทั่วไป (รวมถึงที่แก้ไขเพิ่มเติม)
- การจำแนกข้อมูล (Classify) ให้กำหนดระดับชั้นข้อมูลและเงื่อนไขการเปิดเผยข้อมูลให้สอดคล้องกับความสำคัญของข้อมูล ตามข้อ 7
- การประมวลผลและใช้ข้อมูล (Process/Use) ให้ดำเนินการภายใต้วัตถุประสงค์ที่ได้รับอนุญาต และต้องไม่ขัดต่อกฎหมายหรือสิทธิของเจ้าของข้อมูลส่วนบุคคล
- การเปิดเผยหรือปกปิดข้อมูล (Disclosure/Concealment) ให้ดำเนินการตามสิทธิในการเข้าถึงฐานกฎหมาย และมาตรการคุ้มครองข้อมูลที่กำหนด
- การตรวจสอบข้อมูล (Inspect) ให้สามารถตรวจสอบความถูกต้อง การใช้ข้อมูล และเหตุการณ์ที่เกี่ยวข้องกับข้อมูลได้อย่างครบถ้วน
- การจัดเก็บถาวรหรือการทำลายข้อมูล (Archive/Destroy) ให้ดำเนินการตามระยะเวลาการเก็บรักษา วิธีการทำลาย และการบันทึกการทำลายที่กำหนดไว้ในแนวปฏิบัติว่าด้วยเรื่อง การเก็บ รักษา และ

ทำลายข้อมูลทั่วไป (รวมถึงที่แก้ไขเพิ่มเติม) ทั้งนี้ ห้ามลบหรือทำลายข้อมูลที่อยู่ภายใต้คำสั่งระงับการทำลาย (Legal Hold) ซึ่งออกโดยแผนกกฎหมาย จนกว่าจะมีการยกเลิกคำสั่งเป็นลายลักษณ์อักษร แม้ระยะเวลาการเก็บรักษาตามปกติจะครบกำหนดแล้วก็ตาม

12. การกำหนดสิทธิการเข้าถึงข้อมูล

ให้กำหนดสิทธิการเข้าถึงข้อมูลตามบทบาท หน้าที่ และความจำเป็นในการปฏิบัติงาน โดยกำหนดสิทธิในลักษณะการสร้าง อ่าน แก้ไข และลบข้อมูลตามความเหมาะสม ทั้งนี้ ต้องมีการอนุมัติ ทบทวน และเพิกถอนสิทธิอย่างน้อยปีละ 1 ครั้ง และจัดเก็บบันทึกการเข้าถึงข้อมูลเพื่อประโยชน์ในการตรวจสอบย้อนหลัง

ในกรณีจำเป็นเร่งด่วนที่ไม่สามารถขออนุมัติสิทธิการเข้าถึงตามขั้นตอนปกติได้ทันเวลา เช่น เหตุฉุกเฉินทางธุรกิจ หรือการให้ข้อมูลแก่ผู้ตรวจสอบภายนอก ให้เจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมายสามารถอนุมัติสิทธิการเข้าถึงข้อมูลเป็นการชั่วคราวได้เป็นกรณีไป โดยจำกัดระยะเวลาการเข้าถึงให้เหมาะสม และต้องมีการทบทวนความจำเป็นและความเหมาะสมของการให้สิทธิดังกล่าวภายหลังโดยเร็ว

13. กฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- ประมวลกฎหมายแพ่งและพาณิชย์
- ประมวลกฎหมายอาญา
- ประมวลรัษฎากร
- พระราชบัญญัติการบัญชี พ.ศ. 2543
- พระราชบัญญัติคุ้มครองแรงงาน พ.ศ. 2541
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
- มาตรฐานด้านธรรมาภิบาลข้อมูลที่ใช้บังคับอยู่ในปัจจุบันและที่จะแก้ไขเพิ่มเติมในอนาคต ได้แก่ ISO 38505, ISO 27001 เป็นต้น
- มาตรฐานอื่นที่เกี่ยวข้องกับการบริหารจัดการข้อมูลตามที่บริษัทกำหนด

14. การติดตาม ตรวจสอบ และประเมินผลการปฏิบัติ

ให้คณะทำงานธรรมาภิบาลข้อมูลติดตาม ตรวจสอบ และประเมินผลการปฏิบัติตามนโยบายฉบับนี้อย่างน้อยปีละ 1 ครั้ง รวมถึงการประเมินคุณภาพข้อมูล (Data Quality Assessment: DQA) เพื่อใช้ในการปรับปรุงการดำเนินงานอย่างต่อเนื่อง

15. การสื่อสาร การฝึกอบรม และการสร้างความเข้าใจ

บริษัทส่งเสริมให้บุคลากรทุกระดับมีความรู้ ความเข้าใจ และตระหนักถึงความสำคัญของข้อมูล ผ่านการสื่อสาร การฝึกอบรม และกิจกรรมที่เกี่ยวข้องอย่างต่อเนื่อง

16. การทบทวนและปรับปรุงนโยบาย

ให้คณะทำงานธรรมาภิบาลข้อมูลทบทวนนโยบายฉบับนี้อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมาย ระเบียบ เทคโนโลยี หรือปัจจัยสำคัญอื่นที่เกี่ยวข้อง