ประกาศบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด
เรื่อง นโยบายการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่
(Data Governance and Big Data Management)

---

1. วัตถุประสงค์

เพื่อกำหนดหลักการ หน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้อง ในการกำกับดูแลและบริหารจัดการข้อมูลที่จะช่วยสนับสนุนให้การดำเนินงานเกี่ยวกับข้อมูลมีประสิทธิภาพมากยิ่งขึ้น รวมทั้งป้องกันความเสียหายที่จะเกิดขึ้นกับข้อมูลที่จะส่งผลให้เกิดความเสียหายต่อการดำเนินธุรกิจของ บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด (ธพส.) จึงกำหนดนโยบายการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ เพื่อเป็นแนวทางให้ผู้บริหาร ผู้ปฏิบัติงาน และบุคคลภายนอกถือปฏิบัติได้อย่างถูกต้องเหมาะสม

2. ขอบเขตและการบังคับใช้

ขอบเขตของนโยบายนี้ครอบคลุม ซึ่งครอบคลุมวงจรชีวิตของข้อมูล (Data Life Cycle) และกระบวนการธรรมาภิบาลข้อมูล (Data Governance Process) การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ (Big Data Management) เพื่อให้การจัดการข้อมูลที่มีอยู่และข้อมูลขนาดใหญ่ในอนาคตที่จะเกิดขึ้นมีความถูกต้องและสามารถนำไปประมวลผลเพื่อการตัดสินใจอย่างแม่นยำ สอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของบริษัท การดำเนินงานตามภารกิจของบริษัท และมีผลบังคับใช้ไปถึงบุคลากรหรือหน่วยงานภายในทั้งหมด ได้แก่ กรรมการผู้จัดการ รองกรรมการผู้จัดการ ผู้ช่วยกรรมการผู้จัดการ พนักงานและลูกจ้างของบริษัท ผู้มีส่วนได้ส่วนเสีย

3. ข้อยกเว้น

นโยบายนี้อาจมีการขยายผลหรือมีการยกเว้นโดยปฏิบัติตามขั้นตอนการยกเว้นนโยบายของรัฐด้านอื่น ๆ หรือนโยบายของหน่วยงานร่วมด้วย

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

4. บทบาทและความรับผิดชอบ

บทบาทและความรับผิดชอบกำหนดตามตารางต่อไปนี้

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
คณะกรรมการบริหารจัดการเทคโนโลยีดิจิทัล	คณะกรรมการบริหารจัดการเทคโนโลยีดิจิทัล	ทำหน้าที่พิจารณากลั่นกรอง กำหนดนโยบายและแนวปฏิบัติด้านเทคโนโลยีดิจิทัล
กรรมการผู้จัดการ	กรรมการผู้จัดการ	ทำหน้าที่กำหนดและส่งเสริมนโยบายในการบริหารจัดการข้อมูลที่อยู่ในความครอบครองให้เป็นไปตามหลักธรรมาภิบาลข้อมูล (Data Governance) รวมถึงรับผิดชอบการบริหารจัดการธรรมาภิบาลข้อมูล และสารสนเทศทั้งหมดของ ธพส.
คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council)	คณะกรรมการด้านกำกับดูแลข้อมูลและบริหารจัดการข้อมูลขนาดใหญ่ (Data Governance and Big Data Management)	ทำหน้าที่พิจารณากรอบนโยบายและแนวปฏิบัติด้านกำกับดูแลข้อมูลและบริหารจัดการข้อมูลขนาดใหญ่ เพื่อนำเสนอคณะกรรมการบริหารจัดการเทคโนโลยีดิจิทัลพิจารณา รวมถึง ควบคุม กำกับดูแล และให้คำปรึกษาคณะทำงานที่เกี่ยวข้อง ให้มีการปฏิบัติตามนโยบายและแนวปฏิบัติด้านกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่อย่างเคร่งครัด และกำาหนดให้มีการปรับปรุงนโยบายและแนวปฏิบัติ อย่างน้อยปีละ 1 ครั้ง
ผู้บริหารข้อมูล (Data Executive)	ผู้อำนวยการฝ่ายดิจิทัล	ทำหน้าที่รับผิดชอบการบริหารจัดการข้อมูล ตั้งแต่การเก็บรวบรวม การใช้ การประมวลผล รวมถึงการเปิดเผยข้อมูลที่ได้รับจากทั้งหน่วยงานภายในและหน่วยงานภายนอกตามแนวทางกรอบแนวทางที่คณะทำงานจัดทำธรรมาภิบาลข้อมูลของ ธพส. กำหนด
เจ้าของข้อมูล (Data Owner)	ฝ่ายงานที่เป็นเจ้าของข้อมูล	ทำหน้าที่ตรวจสอบดูแลข้อมูลโดยตรง ทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูล รวมถึงการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล
ผู้สร้างข้อมูล (Data Creators)	บุคคล ฝ่ายงาน คณะทำงานที่เกี่ยวข้อง หรือบุคคลอื่น ๆ ที่สร้างข้อมูล บันทึก แก้ไข ปรับปรุง หรือลบข้อมูล	ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่ถูกกำหนดไว้

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
ผู้ใช้ข้อมูล (Data Users)	บุคคลหรือหน่วยงานทั้งภายในและภายนอก ธพส.	ทำหน้าที่นำข้อมูลไปใช้หรือประมวลผลเพื่อการดำเนินงาน ทั้งในระดับปฏิบัติงาน ระดับบริหาร และสนับสนุนธรรมาภิบาลข้อมูลภาครัฐ โดยการให้ความต้องการในการใช้ข้อมูล
ทีมบริกรข้อมูล (Data Stewards)	คณะทำงานบริกรข้อมูล	ทำหน้าที่รับผิดชอบจัดทำนโยบาย มาตรฐาน เกณฑ์ประเมิน ได้แก่ 1) การกำหนดมาตรฐานเมทาดาตา (Metadata) 2) การบริหารจัดการข้อมูลความมั่นคงปลอดภัยของข้อมูล 3) กำหนดเกณฑ์คุณภาพข้อมูล 4) กำหนดระดับชั้นความลับข้อมูล และวิเคราะห์ ตรวจสอบ แก้ไขปัญหา และสรุปผลการดำเนินงานในแต่ละด้านพร้อมกับข้อเสนอแนะเพื่อเป็นข้อมูลในการจัดทำธรรรมาภิบาลข้อมูลของ ธพส. และผู้เกี่ยวข้อง
ทีมบริหารจัดการข้อมูล (Data Management Team)	คณะทำงานด้านบริหารจัดการข้อมูล	ทำหน้าที่ในการบริหารจัดการข้อมูล สอดคล้องกับ 10 องค์ประกอบ ได้แก่ 1) สถาปัตยกรรมข้อมูล 2) การจำลองและการออกแบบข้อมูล 3) การจัดเก็บและการดำเนินการกับข้อมูล 4) การบูรณาการและความสามารถในการทำงานร่วมกัน 5) การบริหารจัดการเอกสารและเนื้อหา 6) ข้อมูลหลักและข้อมูลอ้างอิง 7) คลังข้อมูล ดาตาเลค ระบบรายงานอัจฉริยะและดาตาอนาไลติกส์ 8) คำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา 9) ความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล 10) คุณภาพของข้อมูลรวมถึงตรวจสอบการปฏิบัติตามนโยบายข้อมูล สนับสนุนกิจกรรมของธรรมาภิบาลข้อมูล เช่น ช่วยเหลือในการนิยามเมทาดาตา (Metadata) ร่างนโยบายข้อมูล เป็นต้น

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
ผู้ควบคุมข้อมูล (Data Controller)	คณะทำงาน คณะกรรมการ ฝ่ายงาน	ทำหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ตามหลักธรรมาภิบาลข้อมูลภาครัฐ หรือตามข้อกำหนดกฎหมายที่เกี่ยวข้อง

5. คำนิยาม

"บริษัท" หมายถึง บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด หรือ เรียกโดยย่อว่า ธพส.

"คณะกรรมการด้านกำกับดูแลข้อมูลและบริหารจัดการข้อมูลขนาดใหญ่ (Data Governance and Big Data Management)" หมายถึง คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) ของ ธพส.

"ผู้บริหารระดับสูงด้านข้อมูล" (Chief Data Officer) หมายถึง ผู้บริหารระดับสูงที่รับผิดชอบด้านการกำกับดูแลข้อมูล

"บุคลากร" หมายถึง กรรมการผู้จัดการ รองกรรมการผู้จัดการ ผู้ช่วยกรรมการผู้จัดการ ผู้อำนวยการฝ่ายที่เกี่ยวข้อง พนักงานและลูกจ้างของ ธพส. หรือผู้ปฏิบัติงานในสังกัด ธพส.

"ธรรมาภิบาลข้อมูลภาครัฐ" หมายถึง การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานของรัฐไปใช้อย่างถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงแลกเปลี่ยนและบูรณาการ ระหว่างกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

"คณะทำงาน" หมายถึง คณะทำงานที่เกี่ยวข้องภายใต้คำสั่งแต่งตั้งบริษัท ซึ่งอยู่ภายใต้อำนาจหน้าที่ของคณะกรรมการด้านกำกับดูแลข้อมูลและบริหารจัดการข้อมูลขนาดใหญ่ ประกอบด้วย (1) คณะทำงานด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Operation Team) (2) คณะทำงานขับเคลื่อนด้านการบริหารจัดการเทคโนโลยีดิจิทัล (3) คณะทำงานด้านจัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์ (Version Control) (4) คณะทำงานบริกรข้อมูล และ (5) คณะทำงานด้านบริหารจัดการข้อมูล

"ผู้บริหาร" หมายถึง กรรมการผู้จัดการ รองกรรมการผู้จัดการ ผู้ช่วยกรรมการผู้จัดการ และผู้อำนวยการฝ่ายที่เกี่ยวข้อง และพนักงานที่มีตำแหน่งตั้งแต่ผู้จัดการส่วน หรือผู้ชำนาญการขึ้นไป

"พนักงาน" หมายถึง บุคคลที่บริษัทตกลงว่าจ้างให้เข้ามาทำงานเป็นการประจำ หรือตามสัญญาจ้างที่มีกำหนดระยะเวลาให้แก่บริษัท โดยได้รับเงินเดือนหรือค่าจ้าง ยกเว้นกรรมการผู้จัดการ ตามพระราชบัญญัติคุ้มครองแรงงานฯ และพนักงานรัฐวิสาหกิจ พ.ศ. 2518 และที่แก้ไขเพิ่มเติม และรองกรรมการผู้จัดการที่มาจากสัญญาจ้าง

"นโยบายข้อมูล Data Policy" หมายถึง หนึ่งในพื้นฐานธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้ธรรมาภิบาลข้อมูลภาครัฐมีประสิทธิภาพจึงกำหนดนโยบายที่สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ คำสั่งหลักเกณฑ์นโยบายและแนวทางปฏิบัติที่เกี่ยวข้อง

"คณะทำงานบริกรข้อมูล (Data Steward)" หมายถึง เจ้าหน้าที่ซึ่งได้รับแต่งตั้งตามคำสั่งของบริษัทปฏิบัติการภายใต้คณะกรรมการด้านกำกับดูแลข้อมูลและบริหารจัดการข้อมูลขนาดใหญ่ (Data Governance and Big Data) และคณะกรรมการด้านคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection)

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

"คณะทำงานด้านบริหารจัดการข้อมูล" หมายถึง เจ้าหน้าที่ซึ่งได้รับแต่งตั้งตามคำสั่งของบริษัท ปฏิบัติการภายใต้คณะกรรมการด้านกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ (Data Governance and Big Data Management) คณะกรรมการด้านคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection) และคณะกรรมการด้านบริหารความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ

"ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล" หมายถึง เจ้าหน้าที่ที่ทำหน้าที่ตรวจสอบดูแลข้อมูลโดยตรง ทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลตามธรรมาภิบาลข้อมูล ตลอดวงจรชีวิตของข้อมูล รวมถึงการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

"ข้อมูล (Data)" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึก โดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจ ระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ และเป็นข้อมูลของบริษัทที่ตั้งอยู่ภายในและภายนอกระบบคอมพิวเตอร์ของบริษัท

"วงจรชีวิตข้อมูล (Data Life Cycle)" หมายถึง ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

"ชุดข้อมูล (Datasets)" หมายถึง การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดข้อมูล ให้ตรงตาม ลักษณะโครงสร้างของข้อมูล

"บัญชีข้อมูล (Data Catalog)" หมายถึง เอกสารแสดงบรรดารายการของชุดข้อมูลที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของ ธพส.

"หมวดหมู่ของข้อมูล (Data Category)" ตามกรอบธรรมาภิบาลข้อมูลภาครัฐแบ่งออกได้เป็น 4 หมวดหมู่ ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง ข้อมูลความลับทางราชการ และ ข้อมูลสาธารณะ

"เมทาดาตา (Metadata)" หมายถึง ข้อมูลที่ใช้กำกับเพื่ออธิบายข้อมูลหรือกลุ่มของข้อมูลอธิบายรายละเอียดของข้อมูลหรือสารสนเทศ ทำให้ทราบรายละเอียดและคุณลักษณะข้อมูล

"ความมั่นคงและปลอดภัยของข้อมูล" หมายถึง ความมั่นคงปลอดภัยของข้อมูล การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้ของข้อมูล รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้าม ปฏิเสธความรับผิด และความน่าเชื่อถือ

"การจัดชั้นความลับของข้อมูล (Data Classification)" หมายถึง การกำหนดประเภทและข้อกำหนดของการจัดชั้นความลับของข้อมูล เพื่อกำหนดสิทธิในการเข้าถึงและสามารถนำข้อมูลไปใช้ได้อย่างเหมาะสม ซึ่งตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 กำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือ ชั้นลับที่สุด โดยคำนึงถึงการปฏิบัติหน้าที่ของบริษัทและประโยชน์แห่งรัฐประกอบกัน ดังนั้น ชั้นความลับของข้อมูลมักถูกกำหนดให้สอดคล้องกับผลกระทบต่อบริษัทและความมั่นคงของประเทศ อาทิ ชื่อเสียง ความต่อเนื่องของการดำเนินงาน การเงิน และทรัพยากรบุคคล

"การบริหารจัดการข้อมูล" หมายถึง ขั้นตอนการสร้างข้อมูล การรวบรวมข้อมูล การจัดเก็บ การจัดเก็บถาวร การทำลายข้อมูล การประมวลผลข้อมูล การใช้ข้อมูลการแลกเปลี่ยน การเชื่อมโยงข้อมูล และการเปิดเผยข้อมูลต่อสาธารณะ

"เจ้าของข้อมูล (Data Owner)" หมายถึง เป็นบุคคลที่ทำหน้าที่รับผิดชอบดูแลข้อมูลโดยตรง สร้างความมั่นใจว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย ทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

"ผู้ควบคุมข้อมูล (Data Controller)" หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้มีสิทธิในการจัดเก็บข้อมูลและทำลายข้อมูล

"ผู้สร้างข้อมูล (Data Creators)" หมายถึง ผู้ใช้ระบบสารสนเทศหรือบริการของ ธพส.

"ผู้บริหารข้อมูล (Data Executive)" หมายถึง ผู้ที่สามารถจัดการข้อมูลและกำหนดสิทธิการเข้าถึงข้อมูล

6. นโยบายและข้อปฏิบัติการบริหารจัดการข้อมูล

การบริหารจัดการข้อมูลประกอบด้วย 7 หัวข้อหลัก ได้แก่

1) ข้อกำหนดทั่วไป
2) การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล (Data Lifecycle Management)
3) คุณภาพข้อมูล (Data Quality)
4) การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange)
5) ความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy)
6) การเปิดเผยข้อมูล (Open Data)
7) มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)

6.1 ข้อกำหนดทั่วไป

<u>วัตถุประสงค์</u>

เพื่อกำหนดแนวทางการดำเนินงานที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของบริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด ในภาพรวมให้เป็นไปด้วยความเรียบร้อย ถูกต้อง รวมทั้งสอดคล้องกับกฎหมายและระเบียบต่าง ๆ ที่เกี่ยวข้อง

<u>แนวทางการปฏิบัติ</u>

1) กำหนดบทบาท หน้าที่ และความรับผิดชอบของแต่ละบุคคลตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้บริหาร พร้อมทั้งกำหนดหน่วยงานเจ้าของข้อมูล เพื่อทำหน้าที่ในการบริหารจัดการข้อมูลนั้น ๆ
2) จัดทำนโยบายการบริหารจัดการข้อมูลเป็นลายลักษณ์อักษร อนุมัติเผยแพร่เพื่อประกาศใช้ และถือปฏิบัติ โดยให้มีผลบังคับใช้กับบุคลากรในบริษัท ตลอดจนหน่วยงาน/บุคคลภายนอกที่เกี่ยวข้องกับการได้มาและการใช้ข้อมูลของบริษัท พร้อมทั้งจัดทำแนวปฏิบัติและมาตรฐานที่เกี่ยวกับข้อมูลเพื่อสนับสนุนการปฏิบัติงานให้สอดคล้องตามนโยบายดังกล่าว ซึ่งประกอบด้วย คุณภาพข้อมูล (Data Quality) การแลกเปลี่ยนและเชื่อมโยงข้อมูล (Data Exchange and Integration) ความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy) การเปิดเผยข้อมูล (Open Data) และมาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)
3) กำหนดมาตรการ วิธีการ และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล โดยปราศจากอำนาจโดยมิชอบหรือโดยมิได้รับอนุญาต (อ้างอิงตามนโยบายความมั่นคงปลอดภัยสารสนเทศของบริษัท หรือเป็นไปตามมาตรฐานสากล)

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๙๓ ๘๘๘๙ www.dad.co.th

4) กำหนดมาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลที่สอดคล้องกับกฎหมาย ระเบียบ และแนวปฏิบัติของหน่วยงาน (อ้างอิงตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) ของบริษัท และเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)
5) ตรวจสอบความมีอยู่และรายละเอียดของข้อมูลที่สำคัญ เช่น คำอธิบายข้อมูลหรือเมทาดาตา ชุดข้อมูล การจัดชั้นความลับข้อมูล และรายงานผลให้แก่ผู้รับผิดชอบตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐและดำเนินการตามกระบวนการธรรมาภิบาลข้อมูลภาครัฐ
6) ตรวจสอบ ติดตาม และประเมินผลการปฏิบัติตามนโยบายการบริหารจัดการข้อมูลโดยผู้ตรวจประเมินที่คณะกรรมการด้านกำกับดูแลข้อมูลและบริหารจัดการข้อมูลขนาดใหญ่ของบริษัทกำหนด พร้อมทั้งกำหนดให้มีการทบทวนนโยบาย รวมถึงมาตรการ วิธีการ และแนวปฏิบัติต่าง ๆ เกี่ยวกับข้อมูล อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญตามความเหมาะสม
7) ตรวจสอบ ติดตาม และประเมินผลการดำเนินงานธรรมาภิบาลข้อมูลของบริษัทอย่างน้อย ปีละ 1 ครั้ง ในเรื่อง (1) การประเมินความพร้อมธรรมาภิบาลข้อมูล (2) การประเมินคุณภาพข้อมูล และ (3) การประเมินความมั่นคงปลอดภัยของข้อมูล เป็นอย่างน้อย (อ้างอิงตามมาตรฐานและหลักเกณฑ์ที่ สพร. กำหนด หรือเป็นไปตามมาตรฐานสากล)
8) จัดให้มีทรัพยากรด้านงบประมาณ ทรัพยากรบุคคล และเทคโนโลยีที่เพียงพอต่อการบริหารจัดการข้อมูล พร้อมทั้งสนับสนุนการฝึกอบรมธรรมาภิบาลข้อมูลภาครัฐและการบริหารจัดการข้อมูลให้ครอบคลุมทั้งวงจรชีวิตของข้อมูลแก่บุคลากรในบริษัท อย่างน้อยปีละ 1 ครั้ง

6.2 การบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล (Data Lifecycle Management)

วัตถุประสงค์

เพื่อกำหนดหลักการและแนวทางการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูลที่สำคัญ ได้แก่ การสร้าง การจัดเก็บข้อมูลและสำรองข้อมูล การใช้ข้อมูลและการประมวลผลข้อมูล การบูรณาการข้อมูล การเปิดเผยข้อมูลและการเชื่อมโยงข้อมูล การจัดเก็บถาวร และการทำลายข้อมูล ได้อย่างมีประสิทธิภาพ มีการรักษาความปลอดภัยของข้อมูล ได้ข้อมูลที่มีคุณภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการนำข้อมูลไปใช้ให้เกิดประโยชน์สูงสุด ทั้งนี้ ควรต้องกำหนดให้มีการจัดทำแนวปฏิบัติในแต่ละกระบวนการของการบริหารจัดการข้อมูลตามวงจรชีวิตข้อมูล

แนวทางการปฏิบัติ

1) กำหนดนโยบาย แนวปฏิบัติ และสภาพแวดล้อมการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล ที่เอื้อต่อการรักษาความมั่นคงปลอดภัย คุ้มครองความเป็นส่วนตัวของข้อมูล และเพื่อให้ได้ข้อมูลที่มีคุณภาพ
2) จัดทำแนวปฏิบัติการจัดการชุดข้อมูล รวมถึงการรักษาความปลอดภัยตามหมวดหมู่และประเภทชั้นความลับตามแนวทางที่เหมาะสม และปรับปรุงอย่างต่อเนื่องให้สอดคล้องกับสถานการณ์
3) จัดเก็บข้อมูลให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้ โดยข้อมูลต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน พร้อมทั้งกำหนดสิทธิและจัดหาระบบ/เครื่องมือที่ใช้ในการเข้าถึงข้อมูลเพื่อรักษาความมั่นคงปลอดภัยและคุณภาพข้อมูล และทำลายข้อมูลตามแนวปฏิบัติและกฎหมายที่เกี่ยวข้อง

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

4) จัดทำแนวปฏิบัติและมาตรฐานการประมวลผลและใช้ข้อมูล เพื่อผู้ใช้นำข้อมูลไปใช้อย่างถูกต้องตามวัตถุประสงค์ที่ต้องการเพื่อให้เกิดประโยชน์สูงสุด
5) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย และแนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม และต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล รวมทั้งจัดให้มีช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย (อ้างอิงตามมาตรฐานและหลักเกณฑ์ที่บริษัทหรือเป็นไปตามมาตรฐานสากล)
6) กำหนดกระบวนการ เทคโนโลยี และมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล และจัดทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้
7) จัดทำแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัย ด้านคุณภาพข้อมูล และด้านคุ้มครองความเป็นส่วนตัวของข้อมูล รวมถึงแนวปฏิบัติให้กับผู้ประสานงาน และตรวจสอบให้แน่ใจว่าได้บริหารจัดการข้อมูลอย่างเหมาะสมตามแนวทางหรือแนวปฏิบัติที่กำหนดไว้
8) สร้างความรู้ความเข้าใจในการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูล ให้แก่ผู้เกี่ยวข้องทั้งภายในและภายนอกหน่วยงาน
9) กำหนดมาตรฐานข้อมูล (Data Standard) ระเบียบปฏิบัติมาตรฐาน และการบริหารจัดการคำอธิบายชุดข้อมูล (Metadata) ให้ครอบคลุมบทบาทหน้าที่ความรับผิดชอบ กระบวนการจัดทำคำอธิบายชุดข้อมูล การควบคุมดูแลและการสอบทานคำอธิบายชุดข้อมูล
10) กำหนดคำนิยามข้อมูล (Data Definition) ขอบเขตข้อมูล (Scope of Data) และลักษณะข้อมูล (Format of Data)

6.3 คุณภาพข้อมูล (Data Quality)

<u>วัตถุประสงค์</u>

เพื่อให้การควบคุมคุณภาพข้อมูลสำหรับการนำไปใช้ประโยชน์ในการบริหารงานและการให้บริการประชาชนเป็นไปตามอำนาจหน้าที่และวัตถุประสงค์ในการดำเนินงานตามที่กฎหมายกำหนด โดยคำนึงถึงคุณภาพข้อมูล (Data Quality) ในทุกชุดข้อมูล (Datasets) ที่ได้ทำการจัดเก็บ

<u>แนวทางการปฏิบัติ</u>

1) กำหนดนโยบายการจัดการคุณภาพข้อมูล เพื่อใช้เป็นกรอบแนวทางในการจัดการข้อมูลของหน่วยงานให้มีคุณภาพเป็นตามเกณฑ์หรือคุณสมบัติที่กำหนด เช่น ความถูกต้องสมบูรณ์ (Accuracy) ความครบถ้วน (Completeness) ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน ความตรงตามความต้องการใช้ (Relevancy) ความน่าเชื่อถือได้ของข้อมูล (Credibility) และความพร้อมใช้ (Availability) เป็นต้น โดยผู้ดูแลข้อมูลมีหน้าที่จัดการและกำกับดูแลข้อมูลให้มีคุณภาพเพื่อสร้างความมั่นใจให้กับผู้ใช้ข้อมูล ในขณะที่ผู้ใช้ข้อมูลมีบทบาทในการให้ข้อเสนอแนะแก่ผู้ดูแลข้อมูลเพื่อการปรับปรุงคุณภาพให้ดียิ่งขึ้น

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

2) จัดทำเกณฑ์คุณภาพข้อมูลที่สามารถวัดผลได้ พร้อมทั้งจัดทำแผนพัฒนาคุณภาพข้อมูลที่สามารถระบุตัวชี้วัดคุณภาพและแผนปฏิบัติการเพื่อจัดการคุณภาพข้อมูลได้อย่างมีประสิทธิภาพ โดยออกแบบการเก็บรวบรวมข้อมูลเพื่อให้ได้ข้อมูลสำหรับประเมินคุณภาพตามเกณฑ์ดังกล่าวให้รวมอยู่ในระบบเทคโนโลยีสารสนเทศและกระบวนการทำงาน (Quality by design) เพื่อลดข้อผิดพลาดและปรับปรุงคุณภาพตั้งแต่จุดการป้อนข้อมูลหรือการสร้างข้อมูลไปจนถึงการประมวลผลข้อมูล (อ้างอิงตามมาตรฐานและหลักเกณฑ์ที่ สพร. หรือเป็นไปตามมาตรฐานสากล)
3) ประเมินผลและจัดการคุณภาพข้อมูลอย่างสม่ำเสมอตลอดวงจรชีวิตของข้อมูล โดยเจ้าของข้อมูลและบริกรข้อมูลควรกำหนดกรอบคุณภาพข้อมูลเฉพาะหมวดหมู่ข้อมูลหรือโดเมน (Domain) เช่น Quality Assurance Framework of the European Statistical System (ESS. QAF) ที่เป็นกรอบคุณภาพข้อมูลสถิติของ the European Statistical System ที่สามารถนำมาใช้อ้างอิงได้
4) พัฒนากระบวนการหรือกลไกให้ผู้ใช้สามารถให้ข้อเสนอแนะหรือ Feedback เพื่อรายงานปัญหาให้กับเจ้าของข้อมูลโดยเฉพาะข้อมูลสำคัญ เช่น ข้อมูลหลัก (Master data) และข้อมูลอ้างอิง (Reference data)
5) กำหนดให้มีการรายงานคุณภาพข้อมูล ประกอบด้วย การกำหนดระดับมิติตัวชี้วัด และค่าเป้าหมายในการประเมินคุณภาพข้อมูล โดยแนบไปกับการใช้ชุดข้อมูล (Datasets) และชุดคำอธิบายข้อมูล
6) จัดให้มีการฝึกอบรมเพื่อสร้างความตระหนักเกี่ยวกับคุณภาพของข้อมูล

6.4 การเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration and Exchange)

วัตถุประสงค์

เพื่อให้การแลกเปลี่ยนข้อมูลทั้งภายในและระหว่างหน่วยงานมีความมั่นคงปลอดภัย และมีคุณภาพสามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีวิธีและแนวทางการนำข้อมูลไปเชื่อมโยงและแลกเปลี่ยนกับหน่วยงานภายนอก ให้สอดคล้องกับระเบียบ หลักเกณฑ์ และกฎหมายที่กำหนดบนพื้นฐานของประโยชน์ส่วนรวมเป็นสำคัญ

แนวทางการปฏิบัติ

1) กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)
2) กำหนดกระบวนการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้ชัดเจน ตั้งแต่ขั้นตอนการเตรียมการ การเริ่มดำเนินการ ระหว่างดำเนินการ และการสิ้นสุดการดำเนินการ
3) กำหนดคำอธิบายชุดข้อมูล (Metadata) ของชุดข้อมูลที่ต้องการเชื่อมโยงและแลกเปลี่ยนที่จำเป็นให้มีความครบถ้วน
4) ทำสัญญาอนุญาตหรือข้อตกลงในการเชื่อมโยงและแลกเปลี่ยนข้อมูล และการนำข้อมูลไปใช้
5) กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการเชื่อมโยงและแลกเปลี่ยนข้อมูล
6) บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Log File) ระหว่างระบบ ทั้งการเชื่อมโยงภายในหน่วยงานและการเชื่อมโยงระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้
7) ตรวจสอบการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้มีการดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติ กระบวนการการเชื่อมโยงและแลกเปลี่ยน และมาตรฐานตามที่กำหนด

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๑๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

8) กำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูล เช่น บุคคลที่ทำหน้าที่ออกแบบกระบวนการและเทคโนโลยีในการเชื่อมโยงและแลกเปลี่ยนข้อมูล (Data Integration Architect) และบุคคลที่ทำหน้าที่ดำเนินการเชื่อมโยงและแลกเปลี่ยนข้อมูลให้สอดคล้องกับที่ได้ออกแบบไว้ (Data Integration Specialist) เป็นต้น

6.5 ความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy)

วัตถุประสงค์

เพื่อกำหนดแนวทางในการบริหารจัดการข้อมูลให้มีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยและความเป็นส่วนบุคคลของข้อมูล

แนวทางการปฏิบัติ

1) จัดทำสถาปัตยกรรมความมั่นคงปลอดภัยของข้อมูล (Data Security Architecture) เพื่อเป็นกรอบในการควบคุม กำกับดูแล และรักษาความมั่นคงปลอดภัยของข้อมูล รวมทั้ง ให้มีการทบทวนสถาปัตยกรรมความมั่นคงปลอดภัยของข้อมูลอย่างสม่ำเสมอ โดยฝ่ายดิจิทัลของ ธพส.
2) กำหนดให้มีการควบคุมการเข้าถึงข้อมูล (Data Access Control) ตามสิทธิ์การเข้าถึงที่คณะกรรมการธรรมาภิบาลกำหนด
3) ตรวจสอบความมั่นคงปลอดภัยของข้อมูล (Data Security Audit) โดยจัดให้มีการตรวจสอบการเข้าถึงข้อมูลตามสิทธิ์ การทดสอบการเจาะระบบสำคัญ รวมทั้ง การตรวจสอบประวัติ (Log) การถูกโจมตีจากผู้ไม่ประสงค์ดีอย่างสม่ำเสมอ
4) กำหนดให้มีการประเมินความปลอดภัยของข้อมูล (Data Security Assessment) โดยทบทวนความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล ประเมินความเสี่ยง วางแผนการป้องกันความเสี่ยง และติดตามการดำเนินงานตามแผนการป้องกันความเสี่ยง
5) จัดหาเครื่องมือและเทคโนโลยีความมั่นคงปลอดภัยของข้อมูล (Data Security Tool /Technology) เพื่อป้องกันและรับมือกรณีที่อาจถูกโจมตีจากผู้ไม่ประสงค์ดีต่ออุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบ หรือโปรแกรมที่อาจจะเกิดความเสียหาย หรือข้อมูลส่วนบุคคลรั่วไหลไปยังบุคคลที่สามโดยไม่ได้รับอนุญาต

6.6 การเปิดเผยข้อมูล (Open Data)

วัตถุประสงค์

เพื่อกำหนดนโยบายข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ สามารถนำกลับมาใช้ใหม่และแจกจ่ายได้โดยใครก็ตาม แต่ต้องระบุแหล่งที่มาหรือเจ้าของงานและต้องใช้สัญญาอนุญาต หรือเงื่อนไขเดียวกันกับที่มาหรือตามเจ้าของข้อมูลกำหนด

แนวทางการปฏิบัติ

1) กำหนดบทบาทหน้าที่ที่เกี่ยวข้องกับการเปิดเผยข้อมูล ได้แก่ กำหนดบุคคล หรือกลุ่มบุคคลที่มีสิทธิ์ตัดสินใจในการเปิดเผยข้อมูล และกำหนดบุคคลหรือกลุ่มบุคคลในการดำเนินการและปรับปรุงการเปิดเผยข้อมูลและกำหนดบุคคลหรือกลุ่มบุคคลในการรับเรื่องและแก้ไขปัญหาเบื้องต้นในการเข้าถึงข้อมูลและการนำข้อมูลไปใช้

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๙๓ ๘๘๘๙ www.dad.co.th

2) ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย และ/หรือแนวปฏิบัติของ ธพส. ในทุกกรณี
3) กำหนดให้การเปิดเผยข้อมูลจำเป็นต้องได้รับการอนุญาตจากเจ้าของข้อมูล (Data Owner)
4) จัดเตรียมข้อมูลตามรูปแบบที่ได้จัดทำไว้เป็นมาตรฐานตามกำหนด และง่ายต่อการนำไปใช้งาน
5) จัดทำคำอธิบายชุดข้อมูล (Metadata) ควบคู่ไปกับข้อมูลที่เปิดเผย
6) ให้มีการคัดเลือกชุดข้อมูลที่ต้องการเผยแพร่ โดยหน่วยงานเจ้าของข้อมูลหรือผู้ที่ได้รับมอบหมาย
7) สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล
8) ต้องปฏิบัติตามอย่างเคร่งครัด และป้องกันมิให้มีการเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต

6.7 มาตรฐานการจัดชั้นความลับข้อมูล (Data Classification Standard)

วัตถุประสงค์

เพื่อให้การประมวลผลข้อมูลและการใช้ข้อมูลเป็นไปอย่างมีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ รวมถึงกำหนดวิธีการและแนวทางในการขอข้อมูลจากหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก เพื่อใช้ประโยชน์ในการปฏิบัติงานและการประมวลผล ทั้งนี้การนำข้อมูลมาใช้ให้เป็นไปตามวัตถุประสงค์ตามที่แจ้ง หากนอกเหนือจากเหตุผลดังกล่าวข้างต้น จะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน

แนวทางการปฏิบัติ

1) กำหนดหมวดหมู่และประเภทชั้นความลับของข้อมูลที่ใช้กับข้อมูลทุกรูปแบบของบริษัท ทั้งเอกสารกระดาษและข้อมูลดิจิทัล ด้วยการประเมินผลกระทบของข้อมูลบริษัท เพื่อระบุหมวดหมู่และประเภทชั้นความลับของข้อมูล รวมทั้งกำหนดระดับความปลอดภัยที่เหมาะสมสำหรับการสร้าง/จัดเก็บ การใช้ และการเข้าถึงชุดข้อมูล และเพื่อใช้กับบุคลากรรวมถึงตัวแทนบุคคลที่สามที่ได้รับอนุญาตให้เข้าถึงข้อมูลในบริษัท พร้อมทั้งกำหนดบทบาทหน้าที่ของบุคลากรในการจัดหมวดหมู่และชั้นความลับ เพื่อป้องกัน จัดการ และกำกับดูแลข้อมูลให้เหมาะสม
2) ติดป้ายกำกับชุดข้อมูล (Labeling/Tagging Dataset) ตามผลประเมินและระบุหมวดหมู่และประเภทชั้นความลับอย่างเหมาะสม และป้ายกำกับสำรองชั้นความลับข้อมูล (ถ้ามี) เช่น ลับ ลับมาก ลับที่สุด เป็นต้น เพื่อจำแนกความแตกต่างของชุดข้อมูลภายในหน่วยงานหรือแนวปฏิบัติตามข้อกำหนดอื่น ๆ
3) กำกับดูแลและติดตามอย่างต่อเนื่อง โดยตรวจสอบความปลอดภัยการใช้งานและรูปแบบการเข้าถึงของระบบและข้อมูล ทั้งผ่านกระบวนการอัตโนมัติหรือโดยบุคคล เพื่อระบุภัยคุกคามภายนอก การบำรุงรักษาการทำงานของระบบตามปกติ และการติดตั้งโปรแกรมเพื่อปรับปรุงและติดตามการเปลี่ยนแปลงของสภาพแวดล้อมของระบบและข้อมูล
4) ต้องมีการเก็บบันทึกประวัติการเข้าถึงและการใช้ข้อมูล (Log Files) เพื่อให้สามารถตรวจสอบย้อนกลับได้
5) กำหนดให้บริกรข้อมูล เจ้าของข้อมูล และผู้มีส่วนได้ส่วนเสียกับข้อมูลที่เกี่ยวข้อง ร่วมกันจัดทำคำอธิบายชุดข้อมูล (Metadata) สำหรับข้อมูลที่จัดเก็บอยู่ในฐานข้อมูล (Database) ในทุกชุดข้อมูล

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

7. ข้อกฎหมายและเอกสารอ้างอิง

1) พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562
2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 2562
3) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
4) พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565
5) พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
6) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ (ราชกิจจานุเบกษา เล่ม 140 ตอนพิเศษ 207 ง วันที่ 29 สิงหาคม 2566) (มรด. 6:2566 มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ)
7) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ (ประกอบด้วย มรด. 3-1:2565 มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการจัดทำบัญชีข้อมูลภาครัฐ และ มรด. 3-2:2565 มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐ)
8) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ เวอร์ชัน 2.0 (ราชกิจจานุเบกษา เล่ม 141 ตอนพิเศษ 261 ง วันที่ 20 กันยายน 2567) (มรด. 8:2567 มาตรฐานรัฐบาลดิจิทัลว่าด้วยแนวทางการเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบดิจิทัลต่อสาธารณะ เวอร์ชัน 2.0)
9) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล (ราชกิจจานุเบกษา เล่ม 140 ตอนพิเศษ 69 ง วันที่ 23 มีนาคม 2566) (ประกอบด้วย มรด. 4-1:2565 มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายการบริหารจัดการข้อมูล และ มรด. 4-2:2565 มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำแนวปฏิบัติการบริหารจัดการข้อมูล)
10) ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ (ราชกิจจานุเบกษา เล่ม 140 ตอนพิเศษ 69 ง วันที่ 23 มีนาคม 2566) (มรด. 5:2565 มาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ)
11) ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม
12) หนังสือสำนักทะเบียนกลาง กรมการปกครอง
13) มสพร. 4-2565 ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูลเรื่องข้อมูลบุคคล เวอร์ชัน 1.0
14) มสพร. 5-2565 ว่าด้วยมาตรฐานการเชื่อมโยงและแลกเปลี่ยนข้อมูลภาครัฐ ด้านความหมายข้อมูลเรื่องข้อมูลนิติบุคคล เวอร์ชัน 1.0
15) มสพร. 3-2565 ว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาภาครัฐเวอร์ชัน 1.0

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๗๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

8. การทบทวนนโยบายข้อมูล

บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด และคณะจัดทำธรรมาภิบาลข้อมูล ทีมบริกรต้องร่วมกันดำเนินการทบทวนนโยบายธรรมาภิบาลข้อมูลเมื่อมีการเปลี่ยนแปลงที่สำคัญหรือตามความเหมาะสม และให้มีการทบทวนนโยบายฉบับนี้อย่างน้อยปีละ 1 ครั้ง

9. ข้อมูลเพิ่มเติม

9.1 การกำหนดประเภทข้อมูล

ประเภทข้อมูล เจ้าของข้อมูลต้องมีการแบ่งประเภทของข้อมูลเพื่อสะดวกในการบริหารจัดการข้อมูลในส่วนที่เกี่ยวข้อง

1) ข้อมูลที่มีโครงสร้าง (Structure Data) เป็นข้อมูลที่มีนิยามโครงสร้างของข้อมูล โดยมีความหมายและคุณสมบัติของแต่ละฟิลด์ข้อมูล โครงสร้างมีร้างมีชั้นเดียว ง่ายต่อการค้นหา เช่น ตารางข้อมูลในฐานข้อมูล เป็นต้น
2) ข้อมูลกึ่งโครงสร้าง (Semi-structure Data) เป็นข้อมูลที่มีนิยามโครงสร้างของข้อมูล แต่ไม่มี Schema ที่ตายตัวหรือเข้มงวด เช่น ข้อมูลที่อยู่ในรูปแบบ Extensible Markup Language - XMl.JavaScript Object Notation - JSON USe Comma-Separated Values - CSV เป็นต้น
3) ข้อมูลไม่มีโครงสร้าง (Unstructured Data) เป็นข้อมูลที่ไม่มีนิยามโครงสร้าง ซึ่งจะอยู่ในรูปแบบ เช่น ข้อความ รูปภาพ เสียง วีดิทัศน์ เป็นต้น

9.2 จัดหมวดหมู่และชั้นความลับของข้อมูล

บริกรข้อมูลและผู้มีส่วนได้เสียกับข้อมูลจะต้องร่วมกันจัดทำนิยามข้อมูล (Data Definition) และ หมวดหมู่ของข้อมูล (Data Category) โดยหมวดหมู่ของข้อมูลจะทำให้ภาพรวมของข้อมูล และการทำเมทาดาตาจะช่วยให้ผู้ใช้ข้อมูลเข้าใจข้อมูลมากยิ่งขึ้น โดยหมวดหมู่ของข้อมูลสามารถถูกแบ่งออกได้เป็น 5 หมวดหมู่ ดังนี้

1) ข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวจนบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)
2) ข้อมูลความมั่นคง (National Security Information) หมายถึง ข้อมูลเกี่ยวกับความมั่นคงของรัฐที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น
3) ข้อมูลความลับ (Classified Information) หมายถึง ข้อมูลที่อยู่ในความครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผยและและมีการกำหนดชั้นความลับของข้อมูล ดังต่อไปนี้
   - **ลับที่สุด** หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญมากที่สุดต่อการดำเนินงานของบริษัท และกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น ที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือมีการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้ โดยไม่ได้รับอนุญาตจะเกิดความเสียหายแก่บริษัทอย่างร้ายแรงที่สุด
   - **ลับมาก** หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญมากต่อการดำเนินงานของบริษัทและกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น ที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือมีการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้ โดยไม่ได้รับอนุญาตจะเกิดความเสียหายแก่บริษัทอย่างร้ายแรง

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๙๓ ๘๘๘๙ www.dad.co.th

- **ลับ** หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญต่อการดำเนินงานของบริษัท และกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น ที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ หากมีการเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือมีการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาตจะเกิดความเสียหายแก่บริษัท

4) ข้อมูลใช้ภายใน (Internal Use Only) หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญต่อการดำเนินงานของบริษัทและเปิดเผยได้เฉพาะภายในบริษัทฯ และบุคคลภายนอกที่มีความสัมพันธ์ทางการค้าเท่านั้น ซึ่งไม่เหมาะที่จะเปิดเผยระดับขั้นนี้โดยไม่ได้รับอนุญาต อาจจะเกิดความเสียหายแก่บริษัท อย่างไรก็ดี ข้อมูลสารสนเทศระดับชั้นนี้จะต้องได้รับการป้องกัน หรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน เพื่อสร้างความเชื่อมั่นให้แก่ผู้ใช้งานรวมทั้งรักษาภาพลักษณ์และชื่อเสียงของบริษัท
5) ข้อมูลทั่วไป (Public Data) หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญทั่วไปต่อการดำเนินงานของบริษัทและเป็นข้อมูลที่สามารถเปิดเผยต่อสาธารณะได้ อย่างไรก็ดี ข้อมูลสารสนเทศในระดับชั้นนี้จะต้องได้รับการป้องกันหรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน เพื่อสร้างความเชื่อมั่นให้แก่ผู้ใช้งาน รวมทั้งรักษาภาพลักษณ์และชื่อเสียงของบริษัท ซึ่งตามนโยบายจะรวมถึงข้อมูลสาธารณะ

ทั้งนี้ ทีมบริกรข้อมูลและผู้มีส่วนได้ส่วนเสียกับข้อมูลจะต้องร่วมกันกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน สำหรับให้ผู้ซึ่งมีหน้าที่เกี่ยวข้องปฏิบัติตามนโยบายหรือกฎเกณฑ์ได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ

9.3 การจัดเก็บและการสำรองข้อมูล

1) ผู้บริหารและผู้รับผิดชอบดูแลข้อมูลสารสนเทศเป็นผู้กำหนดระยะเวลาจัดเก็บข้อมูลสารสนเทศตามระดับความลับ
2) ข้อมูลที่เป็นความลับ หรือมีความสำคัญสูงให้ทำการจัดเก็บแยกไว้ต่างหาก และป้องกันให้มีความปลอดภัยอย่างเพียงพอต่อการเข้าถึง เช่น การทำสัญลักษณ์ลายน้ำและแสดงชั้นความลับกับทุกหน้าของไฟล์ เป็นต้น
3) การทำสำเนาข้อมูลที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากเจ้าของข้อมูล
4) ผู้ปฏิบัติงานต้องทำการป้องกันข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยใช้รหัสผ่านที่มีความมั่นคงปลอดภัย
5) ผู้ปฏิบัติงานทำการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอ หรือตามที่คณะกรรมการกำกับดูแลข้อมูลกำหนด
6) รายงานฝ่ายดิจิทัลทันทีเมื่อข้อมูลสารสนเทศหรืออุปกรณ์ซึ่งบรรจุข้อมูลสารสนเทศสูญหายหรือถูกขโมย

9.4 การเปิดเผยข้อมูล

1) การเผยแพร่ข้อมูลข่าวสารใด ต้องได้รับอนุญาตจากเจ้าของข้อมูลก่อน
2) เจ้าของข้อมูลต้องตรวจสอบความถูกต้องของข้อมูลก่อนอนุญาตนำออกเผยแพร่
3) ผู้ปฏิบัติงานห้ามเปิดเผยข้อมูลลับซึ่งได้มาจากการปฏิบัติงาน ทั้งที่เป็นข้อมูลของบริษัท หรือบุคคลภายนอก

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๙๒ ๒๒๒๒ โทรสาร ๐ ๒๑๙๓ ๘๘๘๙ www.dad.co.th

9.5 การทำลายข้อมูล

ประเภทสื่อบันทึกข้อมูล วิธีการนำสื่อบันทึกกลับมาใช้ใหม่ วิธีการทำลาย

ประเภทสื่อบันทึกข้อมูล	วิธีการนำสื่อบันทึกกลับมาใหม่	วิธีการทำลาย
CD/DVD		ใช้การทุบ หรือทำลายให้เสียหาย
สื่อบันทึกข้อมูลแบบถอดแยกได้ เช่น Flash Drive	ใช้การ Format	ใช้การทุบ หรือทำลายให้เสียหาย
ฮาร์ดดิสก์	ใช้การ Format โดยแบ่งตามระดับชั้นความลับดังนี้ 1) ใช้วิธีเขียนทับซ้ำจำนวน 1 ครั้ง ตามมาตรฐาน NIST 800-88 สำหรับข้อมูลที่เป็นชั้นความลับทั่วไปหรือลับ 2) ใช้วิธีเขียนทับซ้ำจำนวน 3 ครั้ง ตามมาตรฐาน DoD5220.22-M สำหรับข้อมูลที่มีชั้นความลับระดับลับมาก 3) ใช้วิธีเขียนทับซ้ำจำนวน 7 ครั้งตามมาตรฐาน NSA สำหรับข้อมูลที่มีชั้นความลับระดับลับที่สุด	ใช้การทุบ หรือทำลายให้เสียหาย
กระดาษ	ขีดข้อความทิ้งก่อนนำไปใช้เป็นกระดาษ Reuse สำหรับเอกสารที่เป็นชั้นความลับระดับทั่วไป	ใช้เครื่องทำลายเอกสารก่อนทิ้งสำหรับเอกสารที่เป็นชั้นความลับทุกระดับ

1) การบริหารการแลกเปลี่ยนข้อมูลกับบุคคลภายนอก
   - กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจน ตั้งแต่ก่อนดำเนินการ เริ่มดำเนินการ ระหว่างดำเนินการ และสิ้นสุดดำเนินการ
   - ทำงานร่วมกับทีมบริกรข้อมูลเพื่อจัดทำเมทาดาตา (Metadata) ของชุดข้อมูลให้ครบถ้วน และกำหนดเทคโนโลยีรวมถึงมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล
   - จัดทำสัญญาหรือข้อตกลงร่วมกันในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้ตรวจสอบการแลกเปลี่ยนข้อมูลให้เป็นไปตามแนวทาง มาตรฐาน และสัญญาหรือข้อตกลงที่กำหนด

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th

2) การวัดผลการบริหารจัดการข้อมูล

การประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน การประเมินคุณภาพข้อมูล และการประเมินความมั่นคงปลอดภัยของข้อมูล โดยคณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Council) จะต้องจัดตั้งคณะทำงานบริกรข้อมูลที่ประกอบด้วยบริกรข้อมูลจากฝ่ายต่าง ๆ มาออกแบบแผนและวิธีการวัดผลการบริหารจัดการข้อมูล ประเมินความพร้อมของธรรมาภิบาลข้อมูลภาครัฐ ประเมินคุณภาพข้อมูล และประเมินความมั่นคงปลอดภัยของข้อมูล ตรวจสอบผลการดำเนินงานและนำเสนอแนวทางการปรับปรุงแผนและกระบวนการดำเนินงานของทีมบริกรข้อมูล โดยใช้แนวทางการประเมินผลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

ประกาศ ณ วันที่ 24 พฤศจิกายน 2568

(นายนาฬิกอติภัค แสงสนิท)

กรรมการผู้จัดการ

เลขที่ ๑๒๐ อาคารธนพิพัฒน์ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐
โทร. ๐ ๒๑๔๒ ๒๒๒๒ โทรสาร ๐ ๒๑๔๓ ๘๘๘๙ www.dad.co.th