ATLAS ENERGY PUBLIC COMPANY LIMITED

เอกสารสนับสนุน

เรื่อง

แนวปฏิบัติการกำหนดลำดับชั้นความลับของข้อมูล

ประวัติการแก้ไข

02	28 ตุลาคม 2565	- เปลี่ยนหน่วยงานที่รับผิดชอบ จากเดิมเป็น สำนักเลขานุการบริษัท เปลี่ยนเป็นส่วนบริหารความเสี่ยง และเปลี่ยนรหัสหน่วยงานจากเดิม 189000005 เป็น 189000046 - เปลี่ยนรหัสเอกสาร จาก 189000005-SD-021 เป็น 189000046-SD-004 - "แก้ไขหน้า 10 "หน่วยงานสื่อสารองค์กร" เป็น "กรรมการผู้จัดการหรือหน่วยงานที่ได้รับมอบหมาย"
01	24 สิงหาคม 2565	- แปรสภาพบริษัท โดยใช้ชื่อภาษาไทยคือ "บริษัท แอตลาส เอ็นเนอยี จำกัด (มหาชน)" และ ชื่อภาษาอังกฤษคือ "ATLAS ENERGY PUBLIC COMPANY LIMITED"
00	9 กรกฎาคม 2564	จัดทำครั้งแรก
แก้ไขครั้งที่	**วันที่บังคับใช้**	**รายละเอียดการแก้ไข**

แนวปฏิบัติการกำหนดลำดับชั้นความลับของข้อมูล

บทนำ

ข้อมูลนั้นถือว่าเป็นสิ่งที่มีความสำคัญเป็นอย่างมากต่อการปฏิบัติงาน การบริหาร และการจัดการงาน ในทุกระดับขององค์กร ด้วยเหตุดังกล่าวการจัดชั้นความลับข้อมูลสารสนเทศขององค์กรจึงมีความจำเป็นอย่างยิ่ง ซึ่งในการที่จะพิจารณาว่าข้อมูลใดเป็นข้อมูลที่เป็นความลับหรือไม่นั้น ให้พิจารณาถึงความสำคัญของเนื้อหา คุณค่า แหล่งที่มาของข้อมูล วิธีการนำไปใช้ประโยชน์ จำนวนบุคคลที่รับทราบ รวมถึงผลกระทบ และความเสียหายที่อาจจะเกิดขึ้นหากมีการเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาตจากหน่วยงานที่มีหน้าที่รับผิดชอบในฐานะเจ้าของเรื่อง หรือผู้มีอำนาจอนุมัติขององค์กร

วัตถุประสงค์

ข้อมูลถือเป็นทรัพย์สินที่สำคัญของบริษัท ข้อมูลสารสนเทศจะต้องมีการบริหารจัดการอย่างมีประสิทธิภาพ โดยเฉพาะในส่วนของข้อมูลที่เป็นความลับ ซึ่งจะต้องมีการควบคุมการเข้าถึงข้อมูลดังกล่าวไว้อย่างเคร่งครัด เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลโดยมิชอบ หรือโดยไม่ได้รับอนุญาต หรือเพื่อมิให้มีการนำข้อมูลไปเปิดเผยต่อบุคคลหรือถูกเผยแพร่ออกไปโดยมิชอบ หรือไม่ได้รับอนุญาต ซึ่งจะทำให้เกิดความเสี่ยง หรืออาจจะก่อให้เกิดความเสียหายต่อองค์กรในระยะเวลาใดๆ

เอกสารอ้างอิง

189000011-SD-003 : ระเบียบปฏิบัติการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ

189000046-SD-005 : ข้อพึงปฏิบัติทางธุรกิจและจริยธรรมทางธุรกิจของบริษัท

189000046-SD-003 : นโยบายคุ้มครองข้อมูลส่วนบุคคล

นโยบายและคำชี้แจงทั้งหลายขององค์กรเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล

คำจำกัดความ

รายการ	ความหมาย
ข้อมูล	ข้อความ ข่าวสาร เอกสาร เสียง หรือสิ่งอื่นใดที่สามารถสื่อความหมายได้ ที่อยู่ในรูปของตัวเลข ภาษา ภาพ สัญลักษณ์ต่างๆ ที่ยังไม่ผ่านการประมวลผล และผ่านการประมวลผลแล้วทั้งที่อยู่ในรูปอิเล็กทรอนิกส์หรืออยู่ในรูปสิ่งพิมพ์ และให้ความหมายรวมถึง ข้อมูลคอมพิวเตอร์ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ด้วย
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตามคำนิยามของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
ชุดข้อมูล (Data Set)	ข้อมูลที่มีการรวบรวมจัดเป็นชุดไว้ ตามลักษณะโครงสร้างข้อมูลที่กำหนด
คำอธิบายข้อมูล หรือ เมตาดาตา (Data Description or Metadata)	ข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่นๆ ที่เกี่ยวข้องทั้ง กระบวนการเชิงธุรกิจและเชิงเทคโนโลยีสารสนเทศ กฎและข้อจำกัดของข้อมูล และโครงสร้างของข้อมูล คำอธิบายข้อมูลช่วยให้ทุกหน่วยงานสามารถเข้าใจข้อมูล ระบบ และขั้นตอนการทำงานได้ดียิ่งขึ้น ข้อมูลแต่ละชุดควรมีคำอธิบายข้อมูล เพื่อให้ผู้ใช้งานทราบเกี่ยวกับชุดข้อมูล เช่น รายละเอียดชุดข้อมูล สิ่งที่เกี่ยวข้องกับชุดข้อมูล วัตถุประสงค์การนำฟิลด์ข้อมูลไปใช้

รายการ	ความหมาย
ทะเบียนข้อมูล	รายการของชุดข้อมูล ซึ่งสามารถจัดเตรียมได้ในรูปแบบของตาราง รายชื่อชุดข้อมูล รายงาน หรือแอปพลิเคชัน บัญชีข้อมูลถูกใช้เพื่อความสะดวกในการค้นหาชุดข้อมูล (Datasets) หรือคำอธิบายข้อมูล (Metadata)
สื่อบันทึกข้อมูล (Media)	วัสดุหรืออุปกรณ์อิเล็กทรอนิกส์ที่ใช้สำหรับจัดเก็บข้อมูล ในช่วงระยะเวลาหนึ่ง เช่น ฮาร์ดดิสก์ที่เป็นจานหมุนหรือ Solid State ที่อยู่ในเครื่องคอมพิวเตอร์ โน๊ตบุ๊ค แท็บเล็ต อุปกรณ์มือถือ Storage Server Removable Media/Flash Drive แผ่นดิสก์ ม้วนเทป เป็นต้น
องค์กร	บริษัท แอตลาส เอ็นเนอยี จำกัด (มหาชน) และนิติบุคคลอื่นใดที่ บริษัท แอตลาส เอ็นเนอยี จำกัด (มหาชน) เข้าเป็นผู้ถือหุ้นในนิติบุคคลนั้นเกินกว่าร้อยละห้าสิบของจำนวนหุ้นทั้งหมด

การกำกับดูแลข้อมูล

กรรมการผู้จัดการ (CEO) หรือบุคคลที่ได้รับมอบหมาย โดยมอบอำนาจให้ดำเนินการ มีหน้าที่อนุมัติหลักเกณฑ์และแนวปฏิบัติเกี่ยวข้องกับการบริหารจัดการข้อมูล รวมถึงอนุมัติการนำข้อมูลไปใช้ ในกรณีที่กรณีมีข้อสงสัย รวมถึงให้คำปรึกษาและมีอำนาจตัดสินใจที่เกี่ยวข้องกับข้อมูล กำหนดวิธีการประเมินและตรวจวัดการกำกับดูแลข้อมูล

"เจ้าของข้อมูล (Data Owner)" หมายถึง บุคคล ส่วนงาน หรือฝ่ายงานขององค์กรซึ่งมีหน้าที่ดูแลรับผิดชอบในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ตามหน้าที่หรือเพื่อการปฏิบัติงานหรือหน้าที่ในนามขององค์กร โดยเจ้าของระบบงานให้ถือเป็นเจ้าของข้อมูลที่จัดเก็บอยู่ในระบบงานสารสนเทศนั้นด้วย

ในกรณีที่ข้อมูลมีส่วนได้ส่วนเสียข้ามหลายสายงาน ให้สายงานที่มีส่วนได้ส่วนเสียข้อมูลสูงสุดเป็นเจ้าของข้อมูล หรือเสนอต่อกรรมการผู้จัดการ (CEO) หรือบุคคลที่ได้รับมอบหมาย เพื่อพิจารณาอนุมัติหรือดำเนินการใดๆ โดยเจ้าของข้อมูลมีหน้าที่กำหนดชั้นความลับ ควบคุมดูแลข้อมูลที่ตนเป็นเจ้าของ หมายรวมถึงความครบถ้วน ถูกต้อง พร้อมใช้งาน ได้รับการบำรุงรักษาและปกป้องอย่างปลอดภัย อนุมัติการมีสิทธิเข้าถึงและใช้งานข้อมูล รวมถึงการดำเนินการต่าง เช่น การเปลี่ยนแปลง การเปิดเผยข้อมูล ฯลฯ

"ผู้ดูแลข้อมูล" หมายถึง ผู้ที่ได้รับมอบหมายจากเจ้าของข้อมูลให้ดูแลข้อมูลทั้งข้อมูลที่เก็บอยู่ในระบบสารสนเทศและนอกระบบสารสนเทศ เป็นผู้ปฏิบัติหน้าที่ในการจัดเก็บ ดูแล และบำรุงรักษาข้อมูล รวมทั้งการพัฒนาระบบสารสนเทศด้วย

"ผู้สร้างข้อมูล" หมายถึง ผู้ที่ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูล ให้สอดคล้องกับโครงสร้างข้อมูลและวิธีการที่กำหนด เพื่อแก้ไขปัญหาและตรวจสอบด้านคุณภาพข้อมูล รวมถึงความปลอดภัยของผู้ใช้งานข้อมูล

"ผู้ใช้งานข้อมูล" หมายถึง บุคคลที่ทำหน้าที่นำข้อมูลไปใช้งานทั้งในระดับปฏิบัติงานและระดับบริหาร

"เจ้าของข้อมูลส่วนบุคคล (Data Subject)" หมายถึง บุคคลธรรมดาใดๆ ที่องค์กรได้เก็บรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลของบุคคลนั้นไว้ ไม่ว่าจะได้มาจากเจ้าของข้อมูลส่วนบุคคลโดยตรงหรือได้มาจากแหล่งอื่น

"ผู้บริหาร" หมายถึง พนักงานซึ่งดำรงตำแหน่งตั้งแต่ระดับผู้อำนวยการฝ่ายอาวุโสเป็นต้นไป ซึ่งหมายความรวมถึงบุคคลที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบงานของผู้บริหารในแต่ละระดับด้วย เว้นแต่จะระบุไว้เป็นอย่างอื่นในเอกสารฉบับนี้

"หัวหน้าหน่วยงาน" หมายถึง พนักงานซึ่งดำรงตำแหน่งตั้งแต่ระดับผู้จัดการส่วนและผู้อำนวยการฝ่าย ซึ่งหมายความรวมถึงบุคคลที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบงานของหัวหน้าหน่วยงานในแต่ละระดับด้วย เว้นแต่จะระบุไว้เป็นอย่างอื่นในเอกสารฉบับนี้

แนวปฏิบัติการกำหนดลำดับชั้นความลับของข้อมูล

แนวทางปฏิบัติ

เจ้าของข้อมูล และส่วนเทคโนโลยีสารสนเทศ จะต้องกำหนดให้มีการจัดหมวดหมู่ของข้อมูล และทรัพย์สินสารสนเทศที่ใช้ในการดำเนินงานขององค์กร รวมทั้งจะต้องกำหนดลำดับชั้นความลับของข้อมูลและทรัพย์สินสารสนเทศ โดยมีแนวทางปฏิบัติดังนี้

1) จะต้องจัดให้มีการแบ่งระดับชั้นความลับข้อมูลขององค์กร โดยคำนึงถึงระดับความเสี่ยงต่อความมั่นคงปลอดภัยด้านสารสนเทศ ผลกระทบต่อมูลค่า และความเสียหายที่ผู้ใช้บริการ หรือเจ้าของข้อมูลส่วนบุคคลอาจจะได้รับ ซึ่งรวมถึงผลกระทบที่จะก่อให้เกิดความเสียหายต่อทรัพย์สิน และชื่อเสียงทางการค้า หรือการดำเนินธุรกิจขององค์กร ซึ่งข้อมูลขององค์กรนั้นสามารถจะแบ่งระดับความสำคัญเป็น 4 ระดับ ดังนี้

1.1 <u>ข้อมูลที่เผยแพร่ได้ (Public)</u>

เป็นข้อมูลที่องค์กรมีเจตนาต้องการให้ลูกค้า หรือบุคคลภายนอกได้รับทราบ เช่น ข่าวแจกจ่าย (News Release) และแผ่นพับสำหรับโฆษณา (Brochure) ที่ได้ถูกจัดทำออกมาเพื่อการประชาสัมพันธ์ เป็นต้น

1.2 <u>ข้อมูลภายใน (Internal)</u>

เป็นข้อมูลที่องค์กรมีไว้เพื่อให้พนักงานทั่วไปขององค์กรนำไปใช้ในการปฏิบัติงานที่อยู่ในความรับผิดชอบของตนเท่านั้น และองค์กรไม่มีเจตนาต้องการจะให้ลูกค้า หรือบุคคลภายนอกได้รับทราบข้อมูลในส่วนนี้ อย่างไรก็ดี หากได้มีการเผยแพร่ข้อมูลดังกล่าวต่อบุคคลภายนอกแล้วเช่นนี้ก็จะเป็นกรณีที่ไม่ส่งผลกระทบ หรือก่อให้เกิดความเสียหายแก่องค์กรมากนัก ดังนั้น องค์กรโดยส่วนใหญ่ จึงมักจะไม่มีการสร้างมาตรการ หรือระบบการป้องกันการเข้าถึงข้อมูลประเภทนี้ไว้แต่อย่างใด เช่น นโยบายหรือหลักเกณฑ์ที่ใช้ภายใน ระเบียบ, ประกาศ คำสั่ง คู่มือการปฏิบัติงาน บันทึกต่างๆ และจดหมายทั่วไป หรือ Email ที่ส่งภายในบริษัท เป็นต้น

1.3 <u>ข้อมูลลับ (Confidential)</u>

เป็นข้อมูลที่องค์กรมีไว้เพื่อให้แก่เฉพาะพนักงานที่ได้รับมอบหมายนำไปใช้ในการปฏิบัติงานที่อยู่ในความรับผิดชอบ หรือตามที่องค์กรได้มอบหมายไว้เท่านั้น ซึ่งหากถูกนำออกเผยแพร่ไปสู่พนักงานอื่น หรือบุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องแล้วเช่นนี้ ก็จะเป็นกรณีที่ส่งผลกระทบ และก่อให้เกิดความเสียหายแก่องค์กร ลูกค้า พนักงาน หรือบุคคลใดๆ และอาจมีความเสี่ยงที่จะก่อให้เกิดความเสียหาย หรือผลกระทบต่อองค์กรในระดับสูง ดังนั้น จึงมีความจำเป็นจะต้องสร้างมาตรการเก็บรักษา และระบบป้องกันการเข้าถึงข้อมูลประเภทนี้ไว้เพื่อมิให้มีการรั่วไหลออกไปสู่ภายนอก เช่น รายงานทุกประเภทจากระบบคอมพิวเตอร์ ข้อมูลของลูกค้า ข้อมูลส่วนบุคคล และงบประมาณขององค์กร เป็นต้น

1.4 <u>ข้อมูลลับเฉพาะ (Highly Restricted)</u>

เป็นข้อมูลลับที่สำคัญที่สุด ซึ่งหากถูกเผยแพร่ออกไปสู่พนักงานอื่น หรือบุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องแล้วเช่นนี้ ก็เป็นกรณีที่จะส่งผลให้องค์กร ลูกค้า พนักงาน หรือบุคคลใดๆ ต้องเสื่อมเสียชื่อเสียง หรือได้รับการร้องทุกข์กล่าวโทษ หรือถูกฟ้องร้องดำเนินคดี หรือเกิดความเสียหายในประการอื่น เป็นอย่างยิ่ง นอกจากนั้นยังอาจมีความเสี่ยงที่จะก่อให้เกิดความเสียหาย หรือผลกระทบต่อองค์กรในระดับสูงมาก หรือ ข้อมูลที่มีความอ่อนไหวต่อธุรกิจของบริษัท ลูกค้า พนักงาน หรือบุคคลอื่น หรือข้อมูลที่ทำให้สามารถเข้าใช้งานระบบงานหรือเข้าถึงข้อมูลที่ไม่ได้รับอนุญาตของบริษัทได้ ดังนั้น จึงมีความจำเป็นจะต้องสร้างมาตรการเก็บรักษา และระบบป้องกันการเข้าถึงข้อมูลประเภทนี้ไว้อย่างเข้มงวด เช่น ข้อมูลเกี่ยวกับนโยบาย กลยุทธ์ แผนธุรกิจ ผลิตภัณฑ์/บริการใหม่ แผนกลยุทธ์ทางธุรกิจที่บริษัทมีต่อคู่ค้าหรือพันธมิตร หรือแนวทางบริหารจัดการใหม่ขององค์กรที่ยังไม่ถึงเวลาประกาศใช้ ข้อมูลงบการเงินที่ยังไม่ถึงเวลาประกาศ ข้อมูลเกี่ยวกับการควบรวมกิจการ หรือการเพิ่มหรือการลดทุนจดทะเบียนที่ยังไม่ถึงเวลาประกาศ เงินเดือนพนักงาน โบนัสพนักงาน รหัสผ่านของระบบต่างๆ และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) หรือข้อมูลที่มีความอ่อนไหวที่มีความเสี่ยงสูง ซึ่งอาจจะก่อให้เกิดผลกระทบต่อสิทธิเสรีภาพของบุคคลเป็นอย่างมากหากเกิดการรั่วไหลของข้อมูล เป็นต้น

ในกรณีที่ปรากฏว่า ข้อมูลขององค์กรตามข้อ 1.1 ถึงข้อ 1.4 ข้อหนึ่งข้อใด หรือทั้งหมดนั้นมีข้อมูลส่วนบุคคลประกอบรวมอยู่ด้วยแล้วเช่นนี้ เจ้าของข้อมูล และส่วนเทคโนโลยีสารสนเทศจะต้องพิจารณาดำเนินการให้เป็นไปตามนโยบาย และคำชี้แจงเรื่องต่างๆ ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลที่เกี่ยวข้องอย่างเคร่งครัดด้วย

2) จะต้องจัดทำขั้นตอนการปฏิบัติงานเพื่อกำหนดลำดับชั้นความลับ และจัดการทรัพย์สินสารสนเทศขององค์กร โดยให้มีสาระสำคัญครอบคลุมถึงเรื่องต่างๆ ดังต่อไปนี้

2.1 การกำหนดลำดับชั้นความลับข้อมูล

โดยคำนึงถึงระดับความเสี่ยงต่อความมั่นคงปลอดภัยด้านสารสนเทศ ผลกระทบต่อมูลค่าและความเสียหายที่ผู้ใช้บริการ หรือเจ้าของข้อมูลส่วนบุคคลอาจจะได้รับ ซึ่งรวมถึงผลกระทบที่จะก่อให้เกิดความเสียหายต่อทรัพย์สิน และชื่อเสียงทางการค้า หรือการดำเนินธุรกิจขององค์กร

ผู้บริหารของเจ้าของข้อมูล (Data Owner) มีอำนาจ และหน้าที่รับผิดชอบในการกำหนดชั้นความลับข้อมูลรวมถึงอายุการจัดเก็บข้อมูล และจะต้องดำเนินการให้การเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลทั้งหลายเป็นไปตามนโยบาย และคำชี้แจงเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขององค์กรอย่างเคร่งครัด โดยอาจพิจารณามอบหมายให้หัวหน้าหน่วยงานเป็นผู้ปฏิบัติหน้าที่ในส่วนนี้แทนตนได้ตามความเหมาะสม และหากเป็นกรณีที่จำเป็นเร่งด่วนแล้วเช่นนี้ ให้หัวหน้าหน่วยงานที่ได้รับมอบหมายดังกล่าวมีอำนาจกำหนดชั้นความลับเป็นการชั่วคราวได้ โดยในเบื้องต้น ให้หัวหน้ารายงานกรณีดังกล่าวต่อผู้บริหารรับทราบโดยวาจาในทันที และให้รายงานอย่างเป็นลายลักษณ์อักษรให้รับทราบอีกครั้งหนึ่งภายในวันถัดไป เพื่อให้ผู้บริหาร พิจารณาสั่งการในเรื่องต่างๆ ที่เกี่ยวข้องกับการกำหนดชั้นความลับของข้อมูลดังกล่าวให้มีความเหมาะสมโดยเร็วต่อไป ในกรณีที่มีการจัดเก็บข้อมูลหลายระดับชั้นความลับรวมกัน ให้ถือตามชั้นความลับที่สูงสุดของข้อมูล

ในกรณีที่การกำหนดลำดับชั้นความลับข้อมูลขององค์กรนั้น มีความจำเป็นจะต้องอ้างอิงถึงเนื้อหา หรือรายละเอียดของมูลความลับในระดับชั้นที่สูงกว่าไว้ในข้อมูลความลับในระดับที่ต่ำกว่าแล้วเช่นนี้ หัวหน้าหน่วยงานต้องดำเนินการในเรื่องนี้อย่างรอบคอบ และต้องใช้ความระมัดระวังอย่างถึงที่สุด เพื่อมิให้เนื้อหา หรือรายละเอียดของข้อมูลความลับที่มีระดับสูงกว่าต้องถูกเปิดเผย หรือรั่วไหลไปยังลูกค้า พนักงาน หรือบุคคลใดๆ ซึ่งไม่มีหน้าที่เกี่ยวข้องโดยเด็ดขาด

ในกรณีที่ข้อมูลขององค์กรเป็นข้อมูลที่อยู่ในระดับชั้นข้อมูลลับ (Confidential) หรือข้อมูลลับเฉพาะ (Highly Restricted) แล้วเช่นนี้ ส่วนเทคโนโลยีสารสนเทศจะต้องกำหนดสิทธิการอนุมัติการเข้าถึง และการใช้ข้อมูลดังกล่าวในระบบให้กับเจ้าของข้อมูล (Data Owner) โดยกำหนดเงื่อนไขให้หัวหน้าหน่วยงานของส่วนเทคโนโลยีสารสนเทศเป็นผู้มีสิทธิอนุมัติการเข้าถึง และการใช้ข้อมูลดังกล่าว ร่วมกับเจ้าของข้อมูล (Data Owner) ด้วย

2.2 การเปลี่ยนแปลงระดับชั้นความลับของข้อมูล

การเปลี่ยนแปลงระดับชั้นความลับของข้อมูล ไม่ว่าจะเป็นการปรับเพิ่ม ปรับลด หรือยกเลิกระดับชั้นความลับข้อมูลที่เกี่ยวข้องกับหน่วยงานของเจ้าของข้อมูล (Data Owner) นั้น จะต้องแสดงให้เห็นถึงเหตุผล, ความจำเป็น และความเหมาะสมของการที่จะขอให้มีการเปลี่ยนแปลงระดับชั้นของข้อมูลดังกล่าวอย่างเป็นลายลักษณ์อักษรต่อหัวหน้าหน่วยงานของตน ทั้งนี้ ให้ผู้บริหารของเจ้าของข้อมูล (Data Owner) เป็นผู้รับผิดชอบ และมีอำนาจพิจารณาว่า เป็นกรณีที่มีความเหมาะสม และสมควรอนุมัติให้เปลี่ยนแปลงระดับชั้นความลับของข้อมูลตามที่ได้มีการร้องขอมาหรือไม่ ให้ขีดฆ่าชั้นความลับเดิมและระบุชั้นความลับใหม่พร้อมลงนามกำกับในเอกสาร ส่วนข้อมูลอยู่ในรูปแบบอิเล็กทรอนิกส์ ให้ปรับปรุงชั้นความลับที่ระบุใหม่ในทะเบียนข้อมูล

2.3 การกำกับดูแล และการกำหนดมาตรการเกี่ยวกับการใช้ข้อมูล

หมายความรวมถึง แต่ไม่จำกัดแต่เฉพาะเพียงการดำเนินงานในเรื่องต่างๆ ดังนี้

2.3.1 การประทับตรา หรือการจัดทำป้ายแสดงบนสื่อบันทึกข้อมูล

ในกรณีที่การบันทึกข้อมูลความลับขององค์กรได้ถูกกระทำในรูปแบบของ "เอกสาร (Hard Copy)" แล้วเช่นนี้ ให้หน่วยงานซึ่งปีนเจ้าของข้อมูล (Data Owner) จัดทำเครื่องหมายแสดงชั้นความลับของข้อมูล โดยใช้ตัวอักษรสีแดง หรือสีอื่นใดที่มีขนาดใหญ่กว่าปกติ เพื่อให้สามารถสังเกตเห็นได้อย่างชัดเจน โดยให้ระบุข้อความแยกตามชั้นความลับของข้อมูลว่า "ลับ (Confidential)" หรือ "ลับเฉพาะ (Highly Restricted)"

ในส่วนของการบันทึกข้อมูลความลับขององค์กรที่ได้กระทำในรูปแบบของ "ข้อมูลอิเล็กทรอนิกส์" นั้น ให้หน่วยงานซึ่งเป็นเจ้าของข้อมูล (Data Owner) จัดทำเครื่องหมายแสดงชั้นความลับของข้อมูลตามวิธีการเดียวกันกับกรณีของการเก็บข้อมูลในรูปแบบของเอกสาร (Hard Copy) โดยให้ระบุข้อความแยกตามชั้นความลับของข้อมูลไว้ที่ชื่อ Soft File ของข้อมูลในแต่ละประเภทด้วยว่า "ลับ (Confidential)" หรือ "ลับเฉพาะ (Highly Restricted)"

สำหรับข้อมูลภายใน (Internal) ที่มีวัตถุประสงค์เพื่อให้พนักงานทั่วไปขององค์กรนำไปใช้ในการปฏิบัติงานที่อยู่ในความรับผิดชอบของตน และไม่มีเจตนาต้องการจะให้ลูกค้า หรือบุคคลภายนอกได้รับทราบข้อมูลนั้นให้ใช้ตัวอักษรสีแดง หรือสีอื่นใดที่มีขนาดใหญ่กว่าปกติ เพื่อให้สามารถสังเกตเห็นได้อย่างชัดเจน และให้ระบุข้อความว่า "เป็นข้อมูลภายใน ห้ามเผยแพร่ก่อนได้รับอนุญาต (Internal use only)"

นอกจากนี้ให้มีการระบุระยะเวลาจัดเก็บและกำหนดการทำลายข้อมูล เพื่อการบริหารจัดการข้อมูลได้อย่างมีประสิทธิภาพด้วย

2.3.2 การเข้าถึงข้อมูล การจัดทำข้อมูล และสำเนาของข้อมูล

การอ่านข้อมูลที่มีการกำหนดชั้นความลับทุกประเภท การกำหนดสิทธิในระบบที่เกี่ยวกับการ View หรือ Read ข้อมูลดังกล่าวที่ถูกบันทึก หรือเก็บรักษาอยู่ในระบบสารสนเทศ การจัดทำข้อมูลขึ้นใหม่ และการทำสำเนาข้อมูลไม่ว่าทั้งหมด หรือบางส่วน โดยบุคคลใดๆ ที่มิได้เป็นเจ้าของข้อมูล (Data Owner) หรือมิได้เป็นผู้มีอำนาจในการเข้าถึง และจัดทำข้อมูลดังกล่าวนั้น เป็นกรณีที่จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรล่วงหน้าจากหัวหน้าหน่วยงานของเจ้าของข้อมูล (Data Owner) ก่อนที่จะดำเนินการดังกล่าวด้วยทุกครั้ง

การฝ่าฝืนข้อกำหนดในเรื่องนี้ ให้ถือว่าเป็นกรณีของการกระทำความผิดตามกฎหมาย และการกระทำความผิดทางวินัยอย่างร้ายแรง ทั้งในส่วนของผู้ทำการฝ่าฝืน และผู้ที่ได้มีส่วนร่วม หรือเกี่ยวข้องกับการกระทำดังกล่าวด้วยทั้งหมด

2.3.3 การประมวลผลและการใช้งานข้อมูล

การประมวลผลข้อมูลทั้ง ข้อมูลที่นำเข้า วิธีประมวลผล และผลลัพธ์ที่ได้จากการประมวลผล รวมถึงสิทธิในการประมวลผลข้อมูล ต้องได้รับการตรวจสอบความถูกต้องและอนุมัติโดยเจ้าของข้อมูล

ทั้งนี้ ส่วนเทคโนโลยีสารสนเทศ ผู้ดูแลข้อมูลต้องเก็บบันทึกประวัติการประมวลผล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

การให้สิทธิเข้าถึงและใช้งานข้อมูล รวมถึงการนำออกซึ่งข้อมูลจากระบบเพื่อไปใช้งาน ต้องคำนึงถึงระดับชั้นความลับของข้อมูล และความจำเป็นตามบทบาทหน้าที่ของผู้ใช้งานข้อมูล และต้องได้รับการพิจารณาอนุมัติจากเจ้าของข้อมูล

ผู้ใช้งานต้องมีความรับผิดชอบต่อการใช้ข้อมูลของบริษัทอย่างถูกต้องตามบทบาทหน้าที่ และใช้ข้อมูลส่วนบุคคลตามกฎหมาย หรือใช้ตามวัตถุประสงค์ที่มีข้อตกลงหรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล โดยไม่ให้เกิดการสูญเสีย และ/หรือเปิดเผยโดยไม่ได้รับอนุญาต

2.3.4 การเปิดเผย เผยแพร่ การแลกเปลี่ยน หรือการเชื่อมโยงข้อมูล

ในกรณีที่มีความจำเป็นจะต้องส่งมอบ หรือแลกเปลี่ยน หรือเปิดเผยข้อมูลสารสนเทศที่อยู่ในระดับ "ลับ (Confidential)" และ "ลับเฉพาะ (Highly Restricted)" แก่บุคคลภายนอก หรือสาธารณชนแล้วเช่นนี้ ให้ถือปฏิบัติตามแนวทางที่กำหนดไว้ดังต่อไปนี้

(1) หัวหน้าหน่วยงาน และผู้บริหารของเจ้าของข้อมูล (Data Owner) จะต้องใช้ความพยายามอย่างถึงที่สุดในการตรวจสอบความถูกต้องครบถ้วนของข้อมูลดังกล่าว ด้วยความละเอียดรอบคอบ และอย่างถี่ถ้วน โดยจะต้องมีการกำหนดกระบวนการในการแลกเปลี่ยน หรือการเชื่อมโยงข้อมูลให้ชัดเจนตั้งแต่เริ่มต้นจนถึงสิ้นสุดการดำเนินการ (End-to-End Process) เริ่มตั้งแต่ขั้นตอนเตรียมการ เริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ พร้อมทั้งกำหนดคำอธิบายข้อมูล (Data Description) ของชุดข้อมูลที่ต้องการแลกเปลี่ยนให้ครบถ้วน รวมถึงเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

(2) การใช้บริการข้อมูลจากหน่วยงานภายนอก การให้บริการข้อมูลแก่หน่วยงานอื่น และการมีพันธมิตรแบ่งปันและใช้ประโยชน์จากข้อมูลร่วมกัน ต้องมีการประเมินและบริหารความเสี่ยงให้ครอบคลุมถึงการมีสิทธิในข้อมูลโดยชอบด้วยกฎหมาย การรั่วไหลข้อมูล การละเมิดแก้ไขและทำลายข้อมูลที่สำคัญ รวมถึงมีการจัดทำสัญญาข้อตกลงในการแลกปลี่ยนและนำข้อมูลไปใช้ระบุถึงความรับผิดชอบต่อความลับและปลอดภัยของข้อมูล

(3) ต้องมีการบันทึกและจัดเก็บข้อมูลในการดำเนินงานการแลกเปลี่ยนข้อมูลในแต่ละครั้งให้ตรวจสอบย้อนกลับได้

(4) ผู้บริหารของเจ้าของข้อมูล (Data Owner) จะต้องตรวจสอบพบว่าข้อมูลนั้นมีความถูกต้องครบถ้วน โดยข้อมูลที่องค์กรจะส่งมอบ แลกเปลี่ยน เชื่อมโยง หรือเปิดเผยนั้น รวมทั้งข้อมูลส่วนบุคคลและข้อมูลอื่น ในการส่งมอบ หรือการแลกเปลี่ยน หรือการเปิดเผยข้อมูลดังกล่าวจะต้องได้รับการตรวจสอบรายละเอียดและได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลขององค์กรล่วงหน้าก่อนที่จะมีการนำเสนอเรื่องต่อกรรมการผู้จัดการ หรือผู้บริหารที่ได้รับมอบหมายจากบุคคลดังกล่าวเพื่อพิจารณาถึงความเหมาะสมของการที่จะต้องส่งมอบ หรือแลกเปลี่ยน หรือเปิดเผยข้อมูลดังกล่าวด้วยทุกครั้ง

(5) พร้อมกันนี้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลขององค์กร หรือผู้ที่ได้รับมอบหมายจากบุคคลดังกล่าวจะต้องจัดให้บุคคลภายนอกที่จะได้รับมอบ หรือจะได้รับการเปิดเผยข้อมูลเข้าลงนามในข้อตกลงไม่เปิดเผยข้อมูล (Non-Disclosure Agreement หรือ NDA) และสัญญาประมวลผลข้อมูลส่วนบุคคล และ/หรือสัญญาโอนข้อมูลส่วนบุคคล แล้วแต่กรณี รวมถึงจะต้องกำกับดูแลให้ การส่งมอบ การแลกเปลี่ยน การเปิดเผย หรือการเผยแพร่ข้อมูลส่วนบุคคลแก่บุคคลภายนอกดังกล่าว เป็นไปตามที่กำหนดไว้ในนโยบาย หรือคำชี้แจงเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัดอีกด้วย

(6) หากบุคคลภายนอกที่จะได้รับมอบ หรือจะได้รับการเปิดเผยข้อมูลจากองค์กรจะมีการว่าจ้างให้ผู้รับจ้างช่วง (Subcontractor) ของตนทำงานตามสัญญาต่ออีกทอดหนึ่งแล้วเช่นนี้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลขององค์กร หรือผู้ที่ได้รับมอบหมายจากบุคคลดังกล่าวจะต้องกำหนดเงื่อนไขให้บุคคลภายนอกมีหน้าที่ต้องแจ้งให้ห้องค์กรรับทราบ และต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากองค์กรล่วงหน้าเพื่อให้ตนสามารถว่าจ้างบุคคลอื่นให้รับจ้างช่วงต่อไปได้ พร้อมทั้งจะต้องจัดให้ผู้รับจ้างช่วง (Subcontractor) เข้าลงนามในข้อตกลงไม่เปิดเผยข้อมูล (Non-Disclosure Agreement หรือ NDA) และสัญญาประมวลผลข้อมูลส่วนบุคคล และ/หรือสัญญาโอนข้อมูลส่วนบุคคล แล้วแต่กรณี เพิ่มเติมอีกส่วนหนึ่งด้วย

(7) หน่วยงานซึ่งเป็นเจ้าของข้อมูล (Data Owner) จะต้องสร้างรหัสลับ (Encryption) สำหรับการส่งมอบ หรือการแลกเปลี่ยน หรือการเปิดเผยข้อมูลด้วยในทุกๆ ครั้ง

การส่งข้อมูล/ เอกสาร

การปฏิบัติงาน	ลับมาก	ลับ	ใช้ภายใน
การส่งเอกสารด้วยมือ	ต้องใส่ซองปิดผนึกทึบแสง ระบุผู้รับให้ชัดเจน และนำส่งด้วยตนเอง หรือผู้ได้รับมอบหมายจากบริษัทเท่านั้น	ต้องใส่ซองปิดผนึกทึบแสง ระบุผู้รับให้ชัดเจน และนำส่งด้วยตนเอง หรือผู้ได้รับมอบหมายจากบริษัทเท่านั้น	ควรใส่ซองปิดผนึกทึบแสง ระบุผู้รับให้ชัดเจน และนำส่งด้วยตนเอง หรือผู้ได้รับมอบหมายจากบริษัทเท่านั้น
การส่งเอกสารทางไปรษณีย์ หรือผู้ให้บริการภายนอก	ห้ามจัดส่งเอกสารทางไปรษณีย์ ให้ใช้บริษัทผู้ให้บริการที่ธนาคารกำหนดเท่านั้น	กรณีส่งผ่านไปรษณีย์ ต้องส่งแบบปิดผนึกระบุผู้รับอย่างเจาะจง และต้องมีมาตรการป้องกันการรั่วไหลของข้อมูลอื่นเพิ่มเติม เช่น การปิดบังข้อมูลที่สำคัญบางส่วนหรือใช้บริษัทผู้	กรณีส่งผ่านไปรษณีย์ ต้องส่งแบบปิดผนึกระบุผู้รับอย่างเจาะจง และต้องมีมาตรการป้องกันการรั่วไหลของข้อมูลอื่นเพิ่มเติม เช่น การปิดบังข้อมูลที่สำคัญบางส่วนหรือใช้บริษัทผู้

การปฏิบัติงาน	ลับมาก	ลับ	ใช้ภายใน
		ให้บริการที่บริษัทกำหนดเท่านั้น	ให้บริการที่บริษัทกำหนดเท่านั้น
การส่งโทรสาร	ห้ามจัดส่งทางโทรสาร	ต้องแจ้งให้ผู้รับเอกสารรออยู่ที่เครื่องปลายทาง	ควรยืนยันการได้รับเอกสารกับผู้รับ
การส่ง ไฟล์ข้อมูลทางอีเมล์	ต้องมีการเข้ารหัสลับไฟล์ข้อมูล และส่งรหัสแยกจากอีเมล์ที่ส่ง ไฟล์ข้อมูล กรณีเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหว ให้พิจารณาปิดบังข้อมูลบางส่วน (Masking) ก่อนส่ง และพิจารณาแบ่งไฟล์ส่งให้เฉพาะบุคคลที่เกี่ยวข้องโดยตรงเท่านั้น	ต้องมีการเข้ารหัสลับไฟล์ข้อมูล และส่งรหัสแยกจากอีเมล์ที่ส่ง ไฟล์ข้อมูล กรณีเป็นข้อมูลส่วนบุคคล ขอให้พิจารณาปิดบังข้อมูลบางส่วน (Masking) ก่อนส่ง และพิจารณาแบ่งไฟล์ส่งให้เฉพาะบุคคลที่เกี่ยวข้องโดยตรงเท่านั้น	กรณีส่งภายในบริษัทไม่ต้องเข้ารหัส ไฟล์ข้อมูล กรณีส่งไปยังบุคคลภายนอกต้องมีการเข้ารหัสลับไฟล์ข้อมูล การจัดส่งรหัสแยกจากอีเมล์ที่ส่งไฟล์ข้อมูล
การส่ง ไฟล์ข้อมูล ทางช่องทางอิเล็กทรอนิกส์	1) มีการเข้ารหัสลับไฟล์ข้อมูล และส่งรหัสแยกช่องทางจากการส่งไฟล์ข้อมูล หรือ 2) มีมาตรการควบคุมและกำหนดสิทธิ์ในการเข้าถึง **ในกรณีเป็น**ข้อมูลส่วนบุคคลที่มีความอ่อนไหว ให้พิจารณาปิดบังข้อมูลบางส่วน (Masking) ก่อนส่ง และแบ่งไฟล์เพื่อส่งให้เฉพาะบุคคลที่เกี่ยวข้องโดยตรงเท่านั้น เว้นแต่เป็นไปตามรูปแบบข้อมูลที่หน่วยงานราชการกำหนดตามกฎหมาย	1) มีการเข้ารหัสลับไฟล์ข้อมูล และส่งรหัสแยกช่องทางจากการส่งไฟล์ข้อมูล หรือ 2) มีมาตรการควบคุมและกำหนดสิทธิ์ในการเข้าถึง ในกรณีเป็นข้อมูลส่วนบุคคล ให้พิจารณาปิดบังข้อมูลบางส่วน (Masking) ก่อนส่งและแบ่งไฟล์เพื่อส่งให้เฉพาะบุคคลที่เกี่ยวข้องโดยตรงเท่านั้น เว้นแต่เป็นไปตามรูปแบบข้อมูลที่หน่วยงานราชการกำหนดตามกฎหมาย	กรณีส่งภายในบริษัทสามารถดำเนินการได้ โดยไม่ต้องเข้ารหัส ไฟล์ข้อมูล กรณีส่งไปยังบุคคลภายนอกต้อง 1) มีการเข้ารหัส ไฟล์ข้อมูล การจัดส่งรหัสให้แยกช่องทางจากการส่งไฟล์ข้อมูล หรือ 2) มีมาตรการในการควบคุมและกำหนดสิทธิ์ในการเข้าถึง

2.3.5 การจัดเก็บเอกสาร ข้อมูล และสื่อบันทึกข้อมูล

หัวหน้าหน่วยงาน และผู้บริหารของหน่วยงานที่เป็นเจ้าของข้อมูล (Data Owner) จะต้องปฏิบัติ และกำกับดูแลให้เจ้าหน้าที่ภายในหน่วยงานของตนปฏิบัติตามแนวทางเกี่ยวกับการจัดเก็บเอกสาร ข้อมูล และสื่อบันทึกข้อมูลขององค์กร ซึ่งหมายความรวมถึง แต่ไม่จำกัดแต่เฉพาะเพียงการดำเนินงานในเรื่องต่างๆ ดังต่อไปนี้

(1) กำหนดตัวบุคคลผู้มีหน้าที่รับผิดชอบในการจัดเก็บ และ/หรือ เก็บรักษาข้อมูล และสื่อบันทึกข้อมูลไว้อย่างชัดเจน

(2) จะต้องเก็บรักษาข้อมูลในทุกระดับชั้นความลับไว้ในที่ปลอดภัย เพื่อป้องกันการรั่วไหลของข้อมูล ไม่ทิ้งเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลไว้บนโต๊ะทำงาน ห้องประชุม หรือในสถานที่ซึ่งไม่มีผู้ดูแล ไม่ว่าจะเป็นช่วงเวลาที่อยู่ในระหว่างการใช้เอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลนั้นหรือไม่ก็ตาม ในกรณีที่มีความจำเป็นจะต้องหยุดการใช้เอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลเช่นนี้แล้ว เจ้าหน้าที่ผู้เกี่ยวข้องจะต้องนำเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลดังกล่าวไปเก็บไว้ในสถานที่ปลอดภัย เช่น นำไปเก็บไว้ในตู้ หรือลิ้นชัก และใส่กุญแจให้เรียบร้อย เป็นต้น

(3) จะต้องจัดให้มีซึ่งระบบการจัดเก็บเอกสาร ข้อมูล และสื่อบันทึกข้อมูลที่มีประสิทธิภาพ เช่น จัดให้มีกระบวนการแยกแฟ้มเอกสาร และสื่อบันทึกข้อมูลที่อยู่ในชั้นความลับระดับ "ข้อมูลภายใน (Internal)", ระดับ "ลับ (Confidential)" และระดับ "ลับเฉพาะ (Highly Restricted)" และเก็บไว้ในตู้เก็บรักษาข้อมูล ซึ่งถูกปิดด้วยกุญแจที่มีความมั่นคงแยกต่างหากจากเอกสาร ข้อมูล และสื่อบันทึกข้อมูลทั่วไป รวมทั้งจะต้องกำหนดให้มีการจัดทำทะเบียนควบคุมการรับ-ส่งเอกสาร ข้อมูล และสื่อบันทึกข้อมูลในกรณีที่มีการขอยืม หรือขอสำเนาเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลจากหน่วยงานอื่นโดยได้รับอนุญาตเป็นลายลักษณ์อักษรล่วงหน้าจากหัวหน้าหน่วยงานของเจ้าของข้อมูล (Data Owner) แล้ว เป็นต้น

(4) จะต้องเก็บเอกสาร ข้อมูล และสื่อบันทึกข้อมูลออกจากอุปกรณ์ประเภทต่างๆ เช่น เครื่องพิมพ์ เครื่องโทรสาร เครื่องถ่ายเอกสาร เป็นต้น ในทันทีเมื่อได้ใช้งานเอกสาร ข้อมูล และสื่อบันทึกข้อมูลนั้นเรียบร้อยแล้ว โดยต้องไม่เปิด หรือทิ้งเอกสาร ข้อมูล และสื่อบันทึกข้อมูลไว้ในลักษณะที่เป็นการเปิดโอกาส หรืออาจจะทำให้บุคคลที่ไม่มีสิทธิเข้าถึงข้อมูลดังกล่าวสามารถล่วงรู้ข้อมูลที่ปรากฏอยู่ในเอกสาร ข้อมูล หรือสื่อบันทึกข้อมูลได้

(5) จะต้องเก็บเอกสาร ข้อมูล และสื่อบันทึกข้อมูลไว้ในตู้เก็บเอกสาร ข้อมูล และสื่อบันทึกข้อมูลที่มีการควบคุมการเข้าถึงข้อมูล ภายหลังจากเลิกการทำงานของทุกวัน

ในการนี้ เจ้าหน้าที่ผู้ปฏิบัติงานหน่วยงานซึ่งเป็นเจ้าของข้อมูล (Data Owner) จะต้องทำการปิดล็อคตู้เก็บเอกสาร ข้อมูล และสื่อบันทึกข้อมูล เช่น ตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่างๆ เป็นต้น อย่างเหมาะสม และจะต้องมีระบบการเก็บรักษากุญแจที่ใช้สำหรับการปิดล็อคอย่างปลอดภัยด้วย

การปฏิบัติงาน	ลับมาก	ลับ	ใช้ภายใน
การจัดทำป้ายเพื่อระบุชั้นความลับ (Labeling)	ระบุชั้นความลับที่เอกสาร แฟ้มเอกสาร หรือ บันทึกในทะเบียนชุดข้อมูล "ลับเฉพาะ" หรือ "Highly Restricted"	ระบุชั้นความลับที่เอกสาร แฟ้มเอกสาร หรือ บันทึกในทะเบียนชุดข้อมูล เป็น "ลับ" หรือ "Confidential"	แฟ้มเอกสาร แฟ้มเอกสาร หรือ บันทึกในทะเบียนชุดข้อมูล เป็น "ใช้ภายในเท่านั้น" หรือ "Internal Use Only" "เป็นข้อมูลภายใน ห้ามเผยแพร่ก่อนได้รับอนุญาต" หรือ "Internal use only"
การจัดเก็บเอกสาร / สื่อบันทึกข้อมูล	จัดเก็บไว้ในที่ที่มีการควบคุม ป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต เช่น เก็บไว้ในตู้หรือลิ้นชักที่ล็อคกุญแจเมื่อไม่ได้ใช้งาน	จัดเก็บไว้ในที่ที่มีการควบคุม ป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต เช่น เก็บไว้ในตู้หรือลิ้นชักที่ล็อคกุญแจเมื่อไม่ได้ใช้งาน	จัดเก็บภายในบริษัทอย่างเหมาะสม และใช้ความระมัดระวังเมื่อนำออกไปนอกสำนักงาน
การจัดเก็บข้อมูลอิเล็กทรอนิกส์บนระบบงานและสื่อสำรองข้อมูลของระบบงาน	มีการเข้ารหัสลับข้อมูลหรือจำกัดสิทธิ์ในการเข้าถึงหรือจัดเก็บข้อมูลในพื้นที่ที่มีมาตรการควบคุมและจำกัดสิทธิ์ในการเข้าถึง โดยต้องมีการเข้ารหัสลับข้อมูลรหัสผ่าน	มีการเข้ารหัสลับข้อมูลหรือจำกัดสิทธิ์ในการเข้าถึงหรือจัดเก็บข้อมูลในพื้นที่ที่มีมาตรการควบคุมและจำกัดสิทธิ์ในการเข้าถึง	จัดเก็บในไฟล์ข้อมูลที่มีมาตรการควบคุมและจำกัดสิทธิ์ในการเข้าถึง
การจัดเก็บข้อมูลอิเล็กทรอนิกส์บนสื่อบันทึกข้อมูลภายนอกระบบงาน	มีการเข้ารหัสลับข้อมูลและจำกัดสิทธิ์ในการเข้าถึงหรือจัดเก็บข้อมูลในพื้นที่ที่มีมาตรการควบคุมและจำกัดสิทธิ์ในการเข้าถึง	มีการเข้ารหัสลับข้อมูลหรือจำกัดสิทธิ์ในการเข้าถึงหรือจัดเก็บข้อมูลในพื้นที่ที่มีมาตรการควบคุมและจำกัดสิทธิ์ในการเข้าถึง	จัดเก็บในไฟล์ข้อมูลที่มีมาตรการควบคุมและจำกัดสิทธิ์ในการเข้าถึง

(6) ข้อมูลความลับในระดับ "ลับ (Confidential)" และ "ลับเฉพาะ (Highly Restricted)" ที่ถูกเก็บรักษาอยู่ในเครื่องคอมพิวเตอร์ หรือระบบอื่นใดที่คล้ายคลึงกันนั้น จะต้องมีการกำหนดรหัสผ่านเข้าระบบคอมพิวเตอร์เพื่อป้องกันการเข้าถึงข้อมูลดังกล่าวจากบุคคลอื่นที่ไม่มีสิทธิ เพื่อให้เป็นไปตามแนวทางเรื่องการกำหนดรหัสผ่านของ ส่วนเทคโนโลยีสารสนเทศ ด้วยทุกครั้ง

ทั้งนี้ ผู้บริหาร หัวหน้าหน่วยงาน เจ้าหน้าที่ผู้ปฏิบัติงาน และพนักงานทุกคนจะต้องไม่จด หรือบันทึกรหัสผ่านเข้าระบบคอมพิวเตอร์ไว้ในที่ใดๆ ที่บุคคลผู้ไม่มีสิทธิ หรือไม่ได้รับอนุญาตสามารถจะพบเห็นได้ง่ายโดยเด็ดขาด และจะต้องไม่เปิดเผยรหัสผ่านเข้าระบบดังกล่าวให้ผู้อื่นรับทราบอีกด้วย

ในกรณีที่มีการฝ่าฝืนข้อกำหนดเรื่องของการห้ามจดบันทึก หรือห้ามเปิดเผยรหัสผ่านเข้าระบบคอมพิวเตอร์แก่บุคคลอื่นตามข้อ 2.3.4 (6) แล้วเช่นนี้ ให้ถือว่าเป็นกรณีของการกระทำความผิดตามกฎหมาย และการกระทำความผิดทางวินัยอย่างร้ายแรง ทั้งในส่วนของผู้ฝ่าฝืน และผู้ที่ได้มีส่วนร่วม หรือเกี่ยวข้องกับการกระทำดังกล่าวด้วยทั้งหมด

(7) จะต้องไม่ทำการพูดคุย หรือใช้งานข้อมูลในชั้นความลับระดับ "ลับ (Confidential)" และ/หรือ "ลับเฉพาะ (Highly Restricted)" ขององค์กรในบริเวณพื้นที่สาธารณะ หรือ พื้นที่ใดๆ ซึ่งมีความสุ่มเสี่ยงที่อาจจะทำให้บุคคลอื่นสามารถล่วงรู้ถึงข้อมูลดังกล่าวได้โดยเด็ดขาด เช่น ลิฟท์ ร้านอาหาร เป็นต้น

(8) ในกรณีที่เกิดการรั่วไหลของข้อมูลที่อยู่ในชั้นความลับระดับ "ข้อมูลภายใน (Internal)" หรือ "ลับ (Confidential)" หรือ "ลับเฉพาะ (Highly Restricted)" แล้วเช่นนี้ ในเบื้องต้นนั้น หัวหน้าหน่วยงานของเจ้าของข้อมูล (Data Owner) จะต้องรายงานเหตุดังกล่าวโดยวาจาให้ผู้บริหารของหน่วยงานตนรับทราบในทันที และให้รายงานอย่างเป็นลายลักษณ์อักษรให้รับทราบอีกครั้งหนึ่งภายในวันถัดไป เพื่อให้ผู้บริหารพิจารณาสั่งการ และกำหนดแนวทางแก้ไขปัญหาตามความเหมาะสมต่อไป

อย่างไรก็ดี หากการรั่วไหลของข้อมูลที่เกิดขึ้นดังกล่าว เป็นกรณีที่เกี่ยวข้องกับ "ข้อมูลส่วนบุคคล" ไม่ว่าจะเป็นข้อมูลที่อยู่ในชั้นความลับระดับ "ข้อมูลที่เผยแพร่ได้ (Public)" หรือ "ข้อมูลภายใน (Internal)" หรือ "ลับ (Confidential)" หรือ "ลับเฉพาะ (Highly Restricted)" แล้วเช่นนี้ นอกเหนือไปจากการที่หัวหน้าหน่วยงาน และผู้บริหารของเจ้าของข้อมูล (Data Owner) จะต้องถือปฏิบัติให้เป็นไปตามแนวทางที่กำหนดไว้ในข้อ 2.3.4 (8) วรรคแรก แล้วนั้น ในเบื้องต้นนั้น ผู้บริหารของหน่วยงานดังกล่าวจะต้องรายงานเหตุดังกล่าวโดยวาจาให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลรับทราบในทันที และให้รายงานอย่างเป็นลายลักษณ์อักษรให้รับทราบอีกครั้งหนึ่งภายในวันถัดไป เพื่อให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลพิจารณาสั่งการ และกำหนดแนวทางแก้ไขปัญหาตามความเหมาะสมต่อไป

พร้อมกันนี้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะต้องรายงานเหตุดังกล่าวให้กรรมการผู้จัดการรับทราบในทันที หรืออย่างช้าภายใน 24 ชั่วโมง นับแต่เวลาที่ตนได้รับทราบถึงเหตุดังกล่าวเป็นต้นไป

(9) หากการรั่วไหลของข้อมูลนั้น เป็นข้อมูลที่อยู่ในชั้นความลับระดับ "ลับ (Confidential)" หรือ "ลับเฉพาะ (Highly Restricted)" แล้วเช่นนี้ ให้บรรดาผู้เกี่ยวข้องดำเนินการตามแนวทางดังต่อไปนี้

ก. ในกรณีที่ข้อมูลที่รั่วไหลดังกล่าวไม่มีความเกี่ยวข้องกับ "ข้อมูลส่วนบุคคล" แล้วเช่นนี้ ผู้บริหารของหน่วยงานเจ้าของข้อมูล (Data Owner) และผู้บริหารของส่วนเทคโนโลยีสารสนเทศจะต้องร่วมกันแต่งตั้งคณะกรรมการเพื่อสอบสวนข้อเท็จจริง รวมทั้งตรวจสอบ หาสาเหตุของความผิดพลาดที่เกิดขึ้นให้แล้วเสร็จภายใน 3 (สามวัน) และให้นำเสนอผลการพิจารณาต่อกรรมการผู้จัดการ หรือผู้บริหารที่ได้รับมอบหมายจากบุคคลดังกล่าว เพื่อพิจารณาสั่งการในขั้นตอนสุดท้ายต่อไป

ข. กรณีที่ข้อมูลที่รั่วไหลดังกล่าวเป็น "ข้อมูลส่วนบุคคล" ไม่ว่าจะทั้งหมดหรือบางส่วนก็ตาม ผู้บริหารของหน่วยงานเจ้าของข้อมูล (Data Owner) และผู้บริหารของส่วนเทคโนโลยีสารสนเทศจะต้องร่วมกันแต่งตั้งคณะกรรมการเพื่อสอบสวนข้อเท็จจริง และตรวจสอบหาสาเหตุของความผิดพลาดที่เกิดขึ้นให้แล้วเสร็จภายใน 2 (สองวัน) ทั้งนี้ เพื่อที่จะนำเสนอผลการพิจารณาต่อกรรมการผู้จัดการ หรือผู้บริหารที่ได้รับมอบหมายจากบุคคลดังกล่าว เพื่อพิจารณาสั่งการในขั้นตอนสุดท้ายต่อไป ทั้งนี้ คณะกรรมการสอบสวนข้อเท็จจริงที่จะแต่งตั้งขึ้นดังกล่าวจะต้องประกอบด้วยเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล หรือบุคคลที่ได้รับมอบหมายจากบุคคลดังกล่าว เป็นจำนวนอย่างน้อย 1 คน

ในกรณีที่การสอบสวนข้อเท็จจริงได้ผลสรุปว่าเป็นกรณีของการรั่วไหลของข้อมูลในส่วนที่เป็น "ข้อมูลส่วนบุคคล" ด้วยแล้วเช่นนี้ นอกเหนือจากการที่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีหน้าที่จะต้องรายงานเหตุดังกล่าวโดยวาจาให้กรรมการผู้จัดการรับทราบในทันทีตามแนวทางที่กำหนดไว้ในข้อ 2.3.4 (8) วรรคสุดท้าย แล้วนั้น คณะกรรมการสอบสวนข้อเท็จจริง และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในฐานะที่เป็นกรรมการ ยังต้องร่วมกันพิจารณาหาสาเหตุ วิเคราะห์ความเสี่ยง และผลกระทบที่จะเกิดขึ้นแก่เจ้าของข้อมูลส่วนบุคคล รวมทั้งจะต้องกำหนดแนวทางเยียวยาในกรณีที่การรั่วไหล หรือการละเมิดข้อมูลส่วนบุคคลนั้น มีความเสี่ยงสูงที่จะกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล และวิธีการแจ้งเหตุรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลที่เหมาะสมต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลและ/หรือเจ้าของข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง เพิ่มเติมอีกด้วย

นอกจากนั้น หัวหน้าหน่วยงาน และผู้บริหารของหน่วยงานเจ้าของข้อมูล (Data Owner) รวมถึงคณะกรรมการ ผู้บริหารของหน่วยงาน หรือบรรดาผู้เกี่ยวข้องทุกฝ่ายซึ่งมีหน้าที่รับผิดชอบในกรณีนี้จะต้องร่วมกันปรับปรุงวิธีการจัดเก็บข้อมูล จัดให้มีมาตรการการดำเนินการกรณีข้อมูลสูญหาย (Data Loss) หรือข้อมูลรั่วไหล (Data Leak) เพื่อไม่ให้เกิดการรั่วไหลของข้อมูลซ้ำอีก ปรับปรุงระบบการป้องกันการรั่วไหลของข้อมูล และปรับปรุงระบบตรวจสอบย้อนหลังเมื่อมีการรั่วไหลของข้อมูล พร้อมทั้งรายงานผลสรุปของการหารือให้คณะกรรมการและ/หรือกรรมการผู้จัดการ และ/หรือผู้บริหารเกี่ยวข้องรับทราบต่อไป

(10) ห้ามมิให้ผู้บริหาร พนักงาน และบุคคลากรต่างๆ ตอบคำถาม หรือแสดงความเห็นใดๆ ที่เกี่ยวข้องกับข้อมูลขององค์กรในทุกชั้นระดับความลับโดยเด็ดขาด เว้นแต่จะมีหน้าที่เกี่ยวข้องโดยตรงหรือได้รับการมอบหมายอย่างเป็นลายลักษ์อักษรจากองค์กรเพื่อให้มีหน้าที่ในการตอบคำถามดังกล่าวต่อบุคคลใดๆ อย่างไรก็ดี ถึงแม้ว่าผู้บริหาร พนักงาน และบุคคลากรดังกล่าวจะไม่มีหน้าที่ หรือไม่ได้รับมอบหมายให้ตอบคำถามก็ตาม แต่ก็ควรจะต้องแจ้งปฏิเสธต่อผู้ที่สอบถามปัญหาด้วยกิริยาสุภาพ พร้อมทั้งแนะนำให้บุคคลดังกล่าวรอการชี้แจงจากผู้ซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับกรณีนี้ตามข้อปฏิบัติที่องค์กรได้กำหนดไว้ต่อไป

ทั้งนี้ องค์กรได้กำหนดข้อปฏิบัติที่เกี่ยวข้องกับการตอบคำถาม หรือแสดงความเห็นเรื่องข้อมูลขององค์กรสำหรับกรรมการ ผู้บริหาร พนักงาน และบุคคลากรต่างๆ ไว้ดังนี้

ก. กำหนดให้ "กรรมการผู้จัดการ" เป็นผู้มีอำนาจให้สัมภาษณ์ หรือตอบคำถามต่อบรรดาผู้ถือหุ้น นักลงทุน สื่อมวลชน และบุคคลภายนอกแต่เพียงผู้เดียว อย่างไรก็ดี ผู้บริหารระดับสูงขององค์กรท่านอื่นอาจจะให้สัมภาษณ์ หรือตอบคำถามต่อบุคคลดังกล่าวได้ต่อเมื่อได้รับอนุมัติจากกรรมการผู้จัดการเป็นการล่วงหน้าแล้วเท่านั้น

ข. กำหนดให้ "ส่วนนักลงทุนสัมพันธ์" ทำหน้าที่ติดต่อสื่อสารกับบรรดาผู้ถือหุ้น นักลงทุน ผู้จัดการกองทุน สถาบันการเงิน และสายสื่อสารองค์กร เพื่อเป็นการอำนวยความสะดวก และสามารถจะให้ข้อมูลขององค์กรแก่บุคคลดังกล่าวแต่เฉพาะในเรื่องที่ได้รับอนุญาตจากองค์กรเป็นการล่วงหน้าแล้วเท่านั้น

ค. กรณีที่มีบุคคลภายนอกติดต่อสอบถามข้อมูลขององค์กรแล้วเช่นนี้ หากเป็นข้อสอบถามจากบรรดาผู้ถือหุ้น หรือนักลงทุน กำหนดให้ "ส่วนนักลงทุนสัมพันธ์" เป็นผู้ตอบคำถามดังกล่าว แต่หากเป็นข้อสอบถามจากสื่อมวลชน กำหนดให้ "กรรมการผู้จัดการหรือหน่วยงานที่ได้รับมอบหมาย" เป็นผู้ตอบคำถาม

2.3.6 การทำลายสื่อบันทึกข้อมูลก่อนนำกลับมาใช้ใหม่

การทำลายข้อมูลสารสนเทศขององค์กรนั้น จะต้องมีการเสนอต่อเจ้าของข้อมูลเพื่อตรวจสอบการหมดความจำเป็นในการใช้งาน ครบตามระยะเวลาที่กำหนด การหมดอายุการเก็บรักษาตามกฎหมาย เป็นกรณีที่ต้องได้รับอนุมัติจากผู้มีอำนาจอนุมัติตามหลักเกณฑ์อำนาจอนุมัติขององค์กร โดยมีข้อกำหนด และขั้นตอนดังนี้

(1) ต้องจัดทำคำขออนุมัติการทำลายข้อมูล โดยเอกสารดังกล่าวจะต้องถูกเก็บรักษาไว้ในทะเบียนคุมข้อมูลสารสนเทศขององค์กร

(2) เมื่อได้รับคำขออนุมัติการทำลายข้อมูล และผู้บริหารซึ่งเป็นผู้มีอำนาจกำหนดชั้นความลับของหน่วยงานเจ้าของข้อมูลเห็นควรอนุมัติเป็นลายลักษณ์อักษรให้สามารถทำลายข้อมูลตามที่ได้มีการร้องขอแล้วเช่นนี้ ผู้บริหารดังกล่าวจะต้องยกเลิกชั้นความลับของข้อมูลที่ขออนุมัติทำลาย โดยต้องระบุข้อความว่า "ยกเลิกชั้นความลับแล้ว" โดย.....(ผู้บริหารที่มีอำนาจ กำหนดชั้นความลับ) ไว้ที่บริเวณมุมบนด้านขวาของเอกสารข้อมูลความลับในทุกหน้า พร้อมทั้งลงวันที่ เดือน และปี กำกับไว้ในทะเบียนคุมชั้นความลับข้อมูลขององค์กรเพื่อให้สามารถตรวจสอบข้อมูลดังกล่าวได้ในภายหลัง

(3) ข้อมูลสารสนเทศขององค์กรที่ถูกจัดพิมพ์อยู่ในรูปแบบของเอกสาร กระดาษ หรือวัตถุประเภทอื่นใด ซึ่งเป็นข้อมูลที่อยู่ในระดับเอกสารลับ และเอกสารลับเฉพาะนั้นเมื่อไม่ได้นำมาใช้ประโยชน์แล้ว ให้ผู้มีหน้าที่เกี่ยวข้องทำลายข้อมูลดังกล่าวโดยเครื่องทำลายเอกสารเท่านั้น

(4) กรณีที่มีการนำสื่อบันทึกข้อมูลสารสนเทศขององค์กรกลับมาใช้ประโยชน์ใหม่อีกครั้งหนึ่งนั้น ให้ผู้มีหน้าที่เกี่ยวข้องดำเนินการย้ายข้อมูลสารสนเทศที่มีความสำคัญออกไปจากสื่อบันทึกดังกล่าวทั้งหมด พร้อมทั้งให้ดำเนินการลบ Format ของสื่อบันทึกข้อมูลสารสนเทศเป็นการถาวรก่อนที่จะนำกลับมาใช้ใหม่ โดยให้หัวหน้าหน่วยงานของเจ้าของข้อมูลเป็นผู้กำกับดูแล และตรวจสอบความถูกต้องของการดำเนินงานในเรื่องนี้ให้เป็นไปโดยเคร่งครัด ทั้งนี้ เพื่อที่จะเป็นการป้องกันมิให้เกิดการรั่วไหลของข้อมูลดังกล่าว

2.3.7 <u>การทำลายสื่อบันทึกข้อมูลอย่างถาวร</u>

ให้ผู้มีหน้าที่เกี่ยวข้องดำเนินการย้ายข้อมูลสารสนเทศที่มีความสำคัญออกไปจากสื่อบันทึกดังกล่าวทั้งหมด พร้อมทั้งให้ดำเนินการลบ Format ของสื่อบันทึกข้อมูลสารสนเทศเป็นการถาวร เพื่อมั่นใจว่าข้อมูลในเอกสารและสื่อบันทึกข้อมูลจะไม่สามารถกู้คืนกลับมาได้อีก ก่อนที่จะมีการทำลายสื่อบันทึกดังกล่าว

ในการทำลายสื่อบันทึกข้อมูลนั้น จะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารซึ่งเป็นผู้มีอำนาจกำหนดชั้นความลับของหน่วยงานเจ้าของข้อมูลล่วงหน้าแล้วเท่านั้น ในการนี้ ผู้มีหน้าที่เกี่ยวข้องจะต้องทำการเก็บรวบรวมคำสั่งอนุมัติของผู้บริหารดังกล่าวไว้ในบันทึกการปฏิบัติงานในการทำลายข้อมูล (log) เพื่อให้สามารถตรวจสอบข้อมูลได้ในภายหลัง ทั้งนี้ ในการทำลายสื่อบันทึกข้อมูลนั้นจะต้องถูกกระทำภายในพื้นที่เฉพาะ และภายใต้สภาพแวดล้อมที่มีการควบคุมการเข้าถึงของบุคคลอื่นซึ่งไม่มีหน้าที่เกี่ยวข้องไว้อย่างรัดกุม เพื่อเป็นการป้องกันการลักลอบนำสื่อบันทึกข้อมูลดังกล่าวไปใช้ประโยชน์ในทางใดๆ อันอาจจะส่งผลให้เกิดการรั่วไหลซึ่งข้อมูลลับขององค์กรได้ในที่สุด

อนึ่ง การทำลายสื่อบันทึกข้อมูลที่มีข้อมูลส่วนบุคคลรวมอยู่ด้วยนั้นให้เป็นไปตามเงื่อนไขที่กำหนดไว้ในนโยบาย และคำชี้แจงเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขององค์กร

การทำลายเอกสาร และ/หรือสื่อบันทึกข้อมูลที่มีข้อมูลในระดับเป็นความลับก่อนนำกลับมาใช้ใหม่ และการทำลายเอกสาร และ/หรือสื่อบันทึกข้อมูลในระดับเป็นความลับอย่างถาวร

ประเภทสื่อบันทึกข้อมูล	การนำสื่อบันทึกข้อมูล ที่นำกลับมาใช้ใหม่	การทำลายสื่อบันทึกข้อมูลอย่างถาวร
เอกสาร/กระดาษ	ห้ามนำกลับมาใช้ใหม่เป็นกระดาษ reuse และห้ามมิให้ทิ้งลงถังขยะ	ให้ทำลายด้วยเครื่องทำลายเอกสาร
แผ่น CD/DVD	ให้ ลบ/ Format	ให้ทำลายด้วยเครื่องทำลาย CD/DVD หรือทุบทำลาย ทำให้เสียหาย
เทป	ให้ ลบ/ Format	ให้ทำลายด้วยการทุบ หรือทำให้เสียหาย
Hard disk/ Flash Drive	ให้ ลบ/ Format	ให้ทำลายด้วยการทุบ หรือทำให้เสียหาย

เจ้าหน้าที่เทคโนโลยีสารสนเทศต้องจัดทำทะเบียนการทำลาย โดยครอบคลุมอย่างน้อย ผู้รับผิดชอบ วันที่ทำลาย ชนิดของสื่อบันทึกข้อมูล ชั้นความลับของข้อมูลที่อยู่ในสื่อบันทึกข้อมูล Serial number และวิธีการที่ใช้ทำลาย ยกเว้นบางรายการที่ไม่สามารถระบุได้อันเนื่องมาจากสื่อบันทึกข้อมูลชำรุดเสียหายหรือไม่มีข้อมูลปรากฏ และรายงานผลการทำลายสื่อบันทึกข้อมูลต่อผู้บริหารสูงสุดเทคโนโลยีสารสนเทศให้รับทราบ

2.3.8 การจัดการสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้

ในส่วนของสื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาประเภทต่างๆ เช่น PDA, USB-drive, CD - Rom เป็นต้น ซึ่งมีข้อมูลที่อยู่ในระดับชั้นความลับขององค์กรถูกบันทึกอยู่นั้นจะต้องจัดให้มีมาตรการ หรือระบบใดๆ เพื่อป้องกันการเข้าถึงข้อมูลดังกล่าวโดยไม่ได้รับอนุญาต ทั้งนี้เพื่อเป็นการป้องกันการลักลอบนำสื่อบันทึกข้อมูล และข้อมูลดังกล่าวไปใช้ประโยชน์ในทางใดๆ ที่เป็นการผิดวัตถุประสงค์ในระหว่างการเคลื่อนย้ายสื่อบันทึกข้อมูล อันอาจจะส่งผลให้เกิดการรั่วไหลซึ่งข้อมูลลับขององค์กรได้ในที่สุด

การเคลื่อนย้ายสื่อบันทึกข้อมูลดังกล่าวจะต้องถูกดำเนินการโดยเจ้าหน้าที่ผู้รับผิดชอบโดยตรงเท่านั้น และจะต้องกระทำด้วยความระมัดระวังเป็นพิเศษ พร้อมทั้งจะต้องมีการกำหนดมาตรการความปลอดภัยในเรื่องต่างๆ เช่น การป้อนรหัสข้อมูล, การเก็บสำรองข้อมูล, การปิดล็อกหน้าจอของสื่อบันทึกข้อมูลทุกครั้งเมื่อไม่ได้ใช้งาน, การหลีกเลี่ยง หรืองดการใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ, การส่งคืน หรือการทำลายสื่อบันทึกข้อมูลเมื่อสิ้นสุดสภาพการเป็นพนักงาน เป็นต้น ทั้งนี้เพื่อป้องกันการเข้าถึง หรือประมวลผลข้อมูลขององค์กรโดยไม่ได้รับอนุญาต หรือโดยมิชอบ ซึ่งรวมไปถึงการป้องกันมิให้มีการนำข้อมูลความลับขององค์กรไปใช้งานผิดประเภท หรือทำให้ข้อมูลเกิดความเสียหาย

3) จะต้องกำหนดระยะเวลาในการจัดเก็บ และทำลายข้อมูล รวมถึงทรัพย์สินสารสนเทศขององค์กรไว้อย่างเป็นลายลักษณ์อักษร

ผู้บริหารที่มีอำนาจในการกำหนดลำดับชั้นความลับข้อมูล จะต้องกำหนดระยะเวลาของการจัดเก็บและทำลายข้อมูล รวมถึงทรัพย์สินสารสนเทศขององค์กรไว้อย่างเป็นลายลักษณ์อักษร ทั้งนี้ในส่วนของระยะเวลาการจัดเก็บ และทำลายข้อมูลส่วนบุคคลนั้น จะต้องเป็นไปตามที่กำหนดไว้ในนโยบายและคำชี้แจงเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลขององค์กรด้วย

4) จะต้องมีการกำหนดระดับชั้นการอนุมัติ และบริหารจัดการข้อมูลตามลำดับชั้นความลับข้อมูลขององค์กรไว้อย่างเป็นลายลักษณ์อักษร เช่น การขอใช้ข้อมูล การขออนุญาตเข้าถึงข้อมูล หรือการขอทำลายข้อมูล เป็นต้น

การขอใช้ข้อมูล การขออนุญาตเข้าถึงข้อมูล การแลกเปลี่ยนข้อมูลภายในองค์กร การอ่านข้อมูล การทำสำเนาข้อมูลทั้งหมด หรือเพียงบางส่วน การ View ข้อมูลในระบบ การทำลายข้อมูล และการกระทำอื่นใดที่เกี่ยวข้องกับการใช้ประโยชน์ และการเข้าถึงข้อมูลดังกล่าว ("ธุรกรรมสำคัญ") จะสามารถกระทำได้ต่อเมื่อมีการยื่นเรื่องขออนุญาตต่อหน่วยงานผู้เป็นเจ้าของข้อมูล และจะต้องได้รับอนุมัติจากผู้มีอำนาจอนุมัติของหน่วยงานดังกล่าวอย่างเป็นลายลักษณ์อักษรล่วงหน้าแล้วเท่านั้น ทั้งนี้ เพื่อที่จะเป็นการควบคุม และป้องกันความปลอดภัยของข้อมูลดังกล่าว

ในการนี้ ให้กำหนดรายละเอียดเกี่ยวกับบุคคลผู้มีอำนาจอนุมัติไว้ดังนี้

4.1 กรณีที่เป็นข้อมูลที่มีชั้นความลับในระดับ "ลับเฉพาะ (Highly Restricted)"

ในการยื่นเรื่องขออนุญาตทำธุรกรรมสำคัญโดยหน่วยงานผู้ร้องขอนั้น จะต้องได้รับอนุมัติจากผู้บริหารของหน่วยงานผู้ร้องขอ ซึ่งดำรงตำแหน่งตั้งแต่ระดับผู้ช่วยกรรมการผู้จัดการเป็นต้นไป (ซึ่งรวมถึงบุคคลที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบงานของผู้บริหารตั้งแต่ระดับผู้ช่วยกรรมการผู้จัดการ)

เมื่อมีการยื่นเรื่องขออนุญาตทำธุรกรรมสำคัญดังกล่าวโดยหน่วยงานผู้ร้องขอแล้วหน่วยงานผู้ร้องขอจะสามารถทำธุรกรรมสำคัญได้ต่อเมื่อได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหาร ของหน่วยงานที่เป็นเจ้าของข้อมูล ซึ่งดำรงตำแหน่งตั้งแต่ระดับผู้ช่วยกรรมการผู้จัดการเป็นต้นไป (ซึ่งรวมถึงบุคคลที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบงานของผู้บริหารตั้งแต่ระดับผู้ช่วยกรรมการผู้จัดการด้วยแล้วเท่านั้น

กรณีที่การทำธุรกรรมสำคัญนั้นมีความเกี่ยวข้องกับข้อมูลสารสนเทศที่ถูกเก็บรักษาอยู่ในระบบแล้วเช่นนี้ นอกเหนือไปจากการที่จะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารของ หน่วยงานผู้ร้องขอและหน่วยงานที่เป็นเจ้าของข้อมูลตามที่ได้กล่าวไว้แล้วนั้น หน่วยงานผู้ร้องขอจะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารของ ส่วนเทคโนโลยีสารสนเทศ ซึ่งดำรงตำแหน่งตั้งแต่ระดับผู้ช่วยกรรมการผู้จัดการเป็นต้นไป (ซึ่งรวมถึงบุคคลที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบงานของผู้บริหารตั้งแต่ระดับผู้ช่วยกรรมการผู้จัดการ) เพิ่มเติมด้วย

4.2 กรณีที่เป็นข้อมูลที่มีชั้นความลับในระดับ "ลับ (Confidential)"

ในการยื่นเรื่องขออนุญาตทำธุรกรรมสำคัญโดยหน่วยงานผู้ร้องขอนั้นจะต้องได้รับอนุมัติจากผู้บริหารของหน่วยงานผู้ร้องขอ ซึ่งดำรงตำแหน่งตั้งแต่ระดับผู้อำนวยการฝ่ายเป็นต้นไป (ซึ่งรวมถึงบุคคลที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบงานของผู้บริหารตั้งแต่ระดับผู้อำนวยการฝ่าย)

เมื่อมีการยื่นเรื่องขออนุญาตทำธุรกรรมสำคัญดังกล่าวโดยหน่วยงานผู้ร้องขอแล้วหน่วยงานผู้ร้องขอจะสามารถทำธุรกรรมสำคัญได้ต่อเมื่อได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหาร ของหน่วยงานที่เป็น

เจ้าของข้อมูล ซึ่งดำรงตำแหน่งตั้งแต่ระดับผู้อำนวยการฝ่ายเป็นต้นไป (ซึ่งรวมถึงบุคคลที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบงานของผู้บริหารตั้งแต่ระดับผู้อำนวยการฝ่าย) ด้วยแล้วเท่านั้น

กรณีที่การทำธุรกรรมสำคัญนั้นมีความเกี่ยวข้องกับข้อมูลสารสนเทศที่ถูกเก็บรักษาอยู่ในระบบแล้วเช่นนี้ นอกเหนือไปจากการที่จะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารของ หน่วยงานผู้ร้องขอและหน่วยงานที่เป็นเจ้าของข้อมูลตามที่ได้กล่าวไว้แล้วนั้น หน่วยงานผู้ร้องขอจะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารของส่วนเทคโนโลยีสารสนเทศ ซึ่งดำรงตำแหน่งตั้งแต่ระดับผู้อำนวยการฝ่ายเป็นต้นไป (ซึ่งรวมถึงบุคคลที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบงานของผู้บริหารตั้งแต่ระดับผู้อำนวยการฝ่าย) เพิ่มเติมด้วย

4.3 <u>กรณีที่เป็น "ข้อมูลภายใน (Internal)"</u>

ในการยื่นเรื่องขออนุญาตทำธุรกรรมสำคัญโดยหน่วยงานผู้ร้องขอนั้น จะต้องได้รับอนุมัติจากผู้บริหารของหน่วยงานผู้ร้องขอ ซึ่งดำรงตำแหน่งตั้งแต่ระดับผู้จัดการส่วนเป็นต้นไป (ซึ่งรวมถึงบุคคลที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบงานของผู้บริหารตั้งแต่ระดับผู้จัดการส่วน)

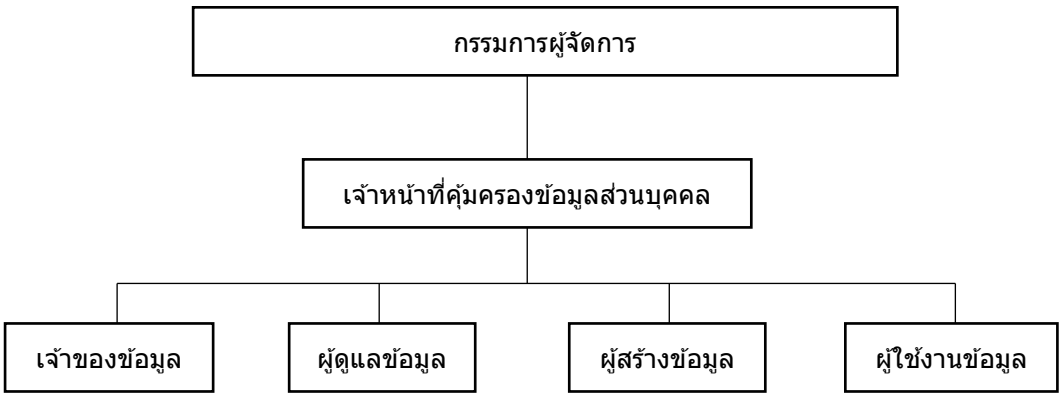
เมื่อมีการยื่นเรื่องขออนุญาตทำธุรกรรมสำคัญดังกล่าวโดยหน่วยงานผู้ร้องขอแล้วหน่วยงานผู้ร้องขอจะสามารถทำธุรกรรมสำคัญได้ต่อเมื่อได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารของหน่วยงานที่เป็นเจ้าของข้อมูล ซึ่งดำรงตำแหน่งตั้งแต่ระดับผู้จัดการส่วนเป็นต้นไป (ซึ่งรวมถึงบุคคลที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบงานของผู้บริหารตั้งแต่ระดับผู้จัดการส่วน) ด้วยแล้วเท่านั้น

กรณีที่การทำธุรกรรมสำคัญนั้นมีความเกี่ยวข้องกับข้อมูลสารสนเทศที่ถูกเก็บรักษาอยู่ในระบบแล้วเช่นนี้ นอกเหนือไปจากการที่จะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารของหน่วยงานผู้ร้องขอและหน่วยงานที่เป็นเจ้าของข้อมูลตามที่ได้กล่าวไว้แล้วนั้น หน่วยงานผู้ร้องขอจะต้อง ได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บริหารของ ส่วนเทคโนโลยีสารสนเทศ ซึ่งดำรงตำแหน่งตั้งแต่ระดับผู้จัดการส่วนเป็นต้นไป (ซึ่งรวมถึงบุคคลที่ได้รับมอบหมายให้เป็นผู้รับผิดชอบงานของผู้บริหารตั้งแต่ระดับผู้จัดการส่วน) เพิ่มเติมด้วย

ในการพิจารณาอนุมัติให้สิทธิทำธุรกรรมสำคัญดังกล่าวนั้น หน่วยงานที่เป็นเจ้าของข้อมูลจะต้องให้สิทธิดังกล่าวแก่หน่วยงานที่ร้องขอภายในขอบเขตจำกัด และเท่าที่มีความจำเป็นต่อการปฏิบัติงานเท่านั้น

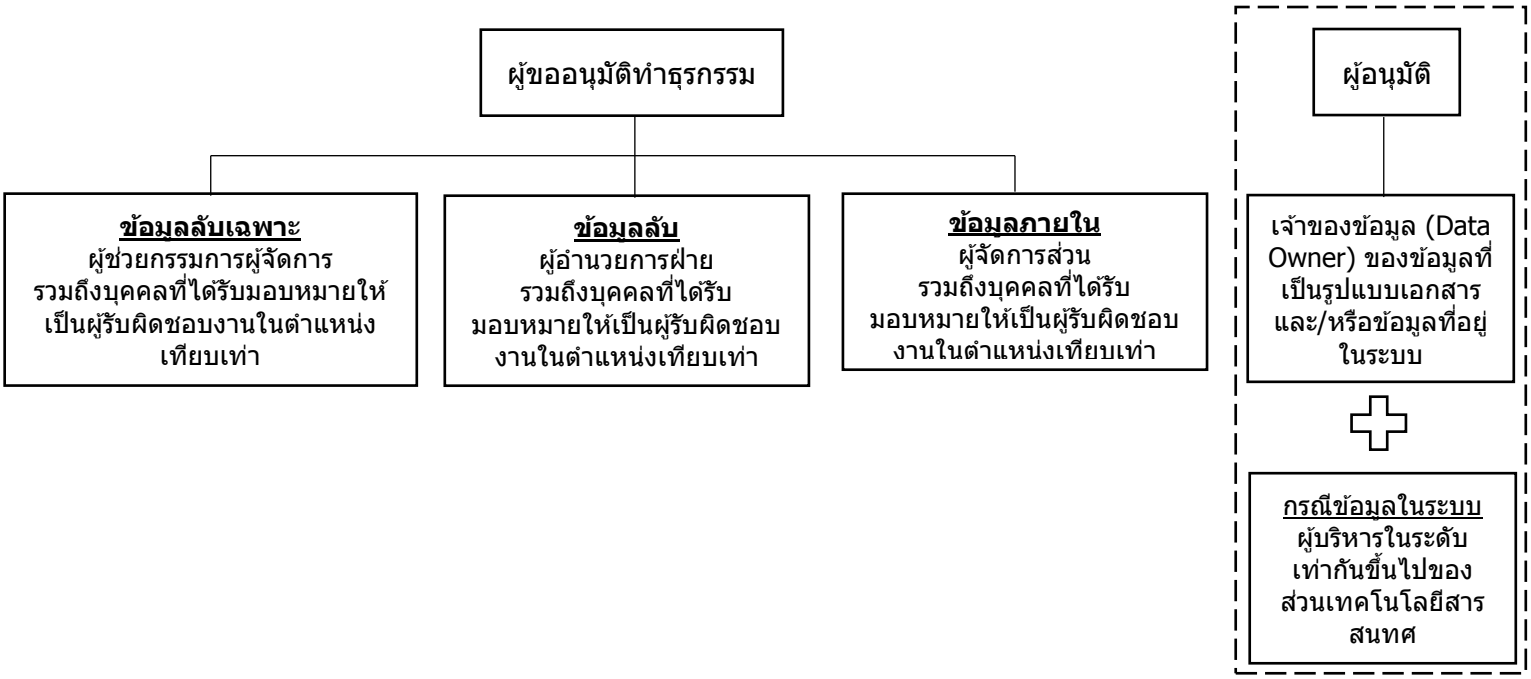
ในการรับ และ/หรือส่งข้อมูล และ/หรือ Electronic File ที่เป็นความลับระหว่างหน่วยงานภายในองค์กร หรือภายนอกองค์กรนั้น จะต้องมีการเข้ารหัสข้อมูล หรือกำหนดสิทธิในการเข้าถึงข้อมูลด้วยทุกครั้ง

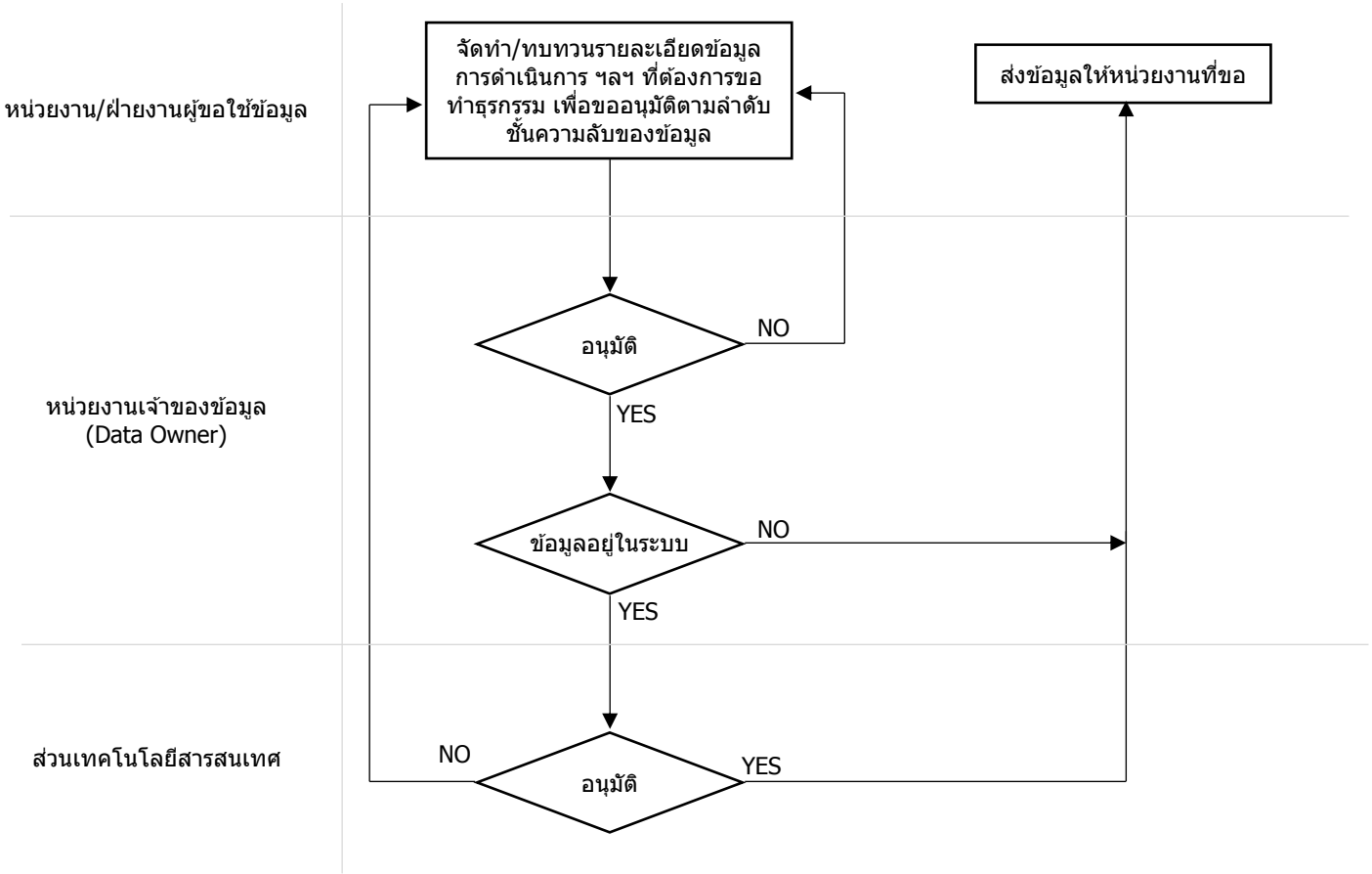
โครงสร้างการกำกับดูแลข้อมูลภายในที่เกี่ยวกับขอข้อมูลส่วนบุคคล
รวมถึงกรณีขออนุมัติข้อมูลที่ต้องเปิดเผยต่อบุคคลภายนอก



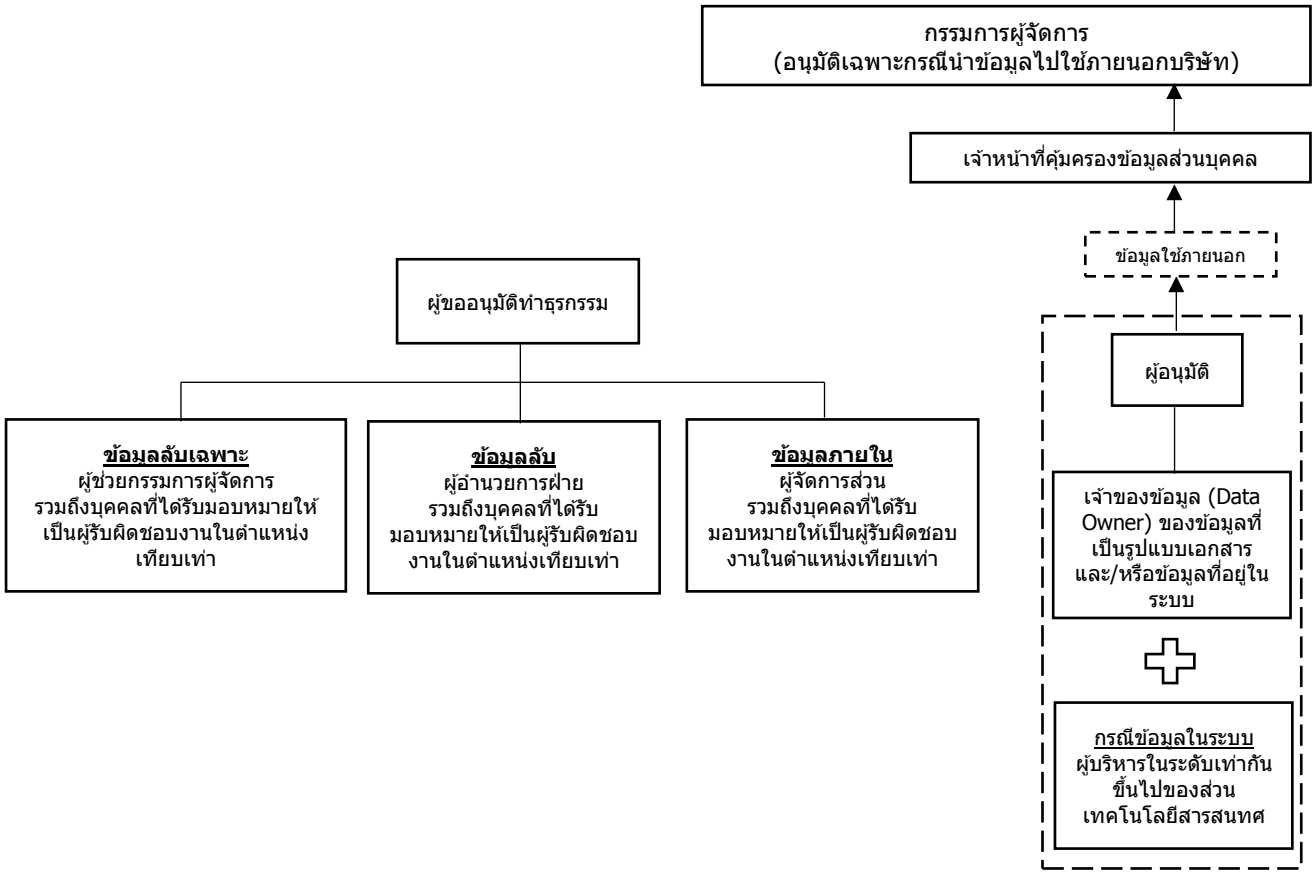
แนวปฏิบัติการกำหนดลำดับชั้นความลับของข้อมูล

การขออนุมัติใช้ข้อมูลภายใน

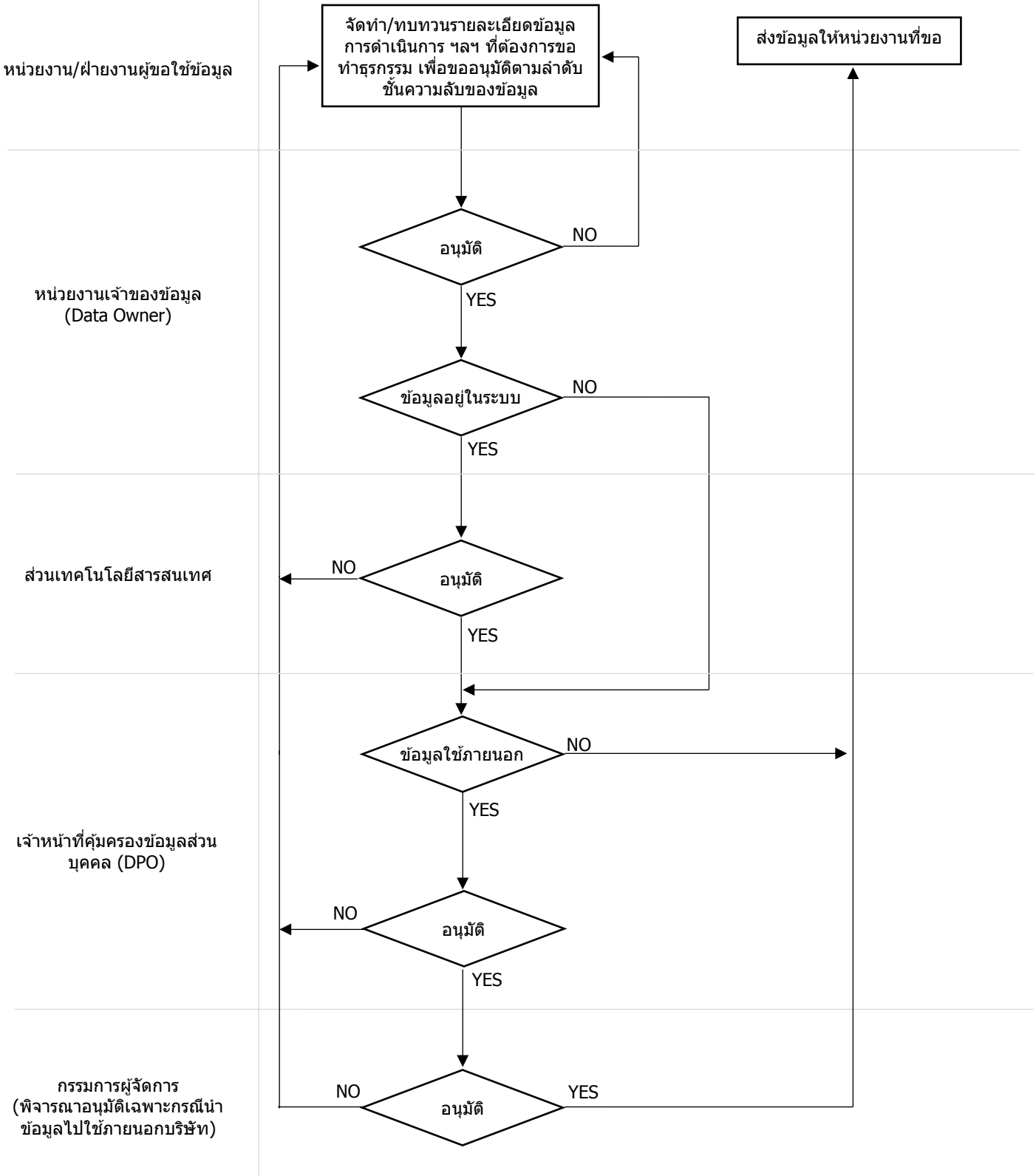




การขออนุมัติใช้ข้อมูลส่วนบุคคล
รวมถึงกรณีข้อมูลที่ต้องเปิดเผยต่อบุคคลภายนอก



แนวปฏิบัติการกำหนดลำดับชั้นความลับของข้อมูล



เอกสารแนบ

ข้อมูลลับเฉพาะ

No.	ประเภท/ ลักษณะข้อมูล	หน่วยงานผู้จัดทำข้อมูล	หน่วยงานผู้ใช้ข้อมูล (Data User)	หน่วยงานเจ้าของข้อมูล (Data Owner)	เก็บในระบบ
	ข้อมูลลูกค้า				
1	ข้อมูลพฤติกรรมการใช้งานของลูกค้า	ส่วนการตลาด	ส่วนการตลาด	ส่วนการตลาด	CRM
2	ข้อมูลลูกค้าใช้แคมเปญ	ส่วนการตลาด	ส่วนการตลาด	ส่วนการตลาด	CRM
	ข้อมูลผู้บริหาร/พนักงาน				
3	ข้อมูลเงินเดือนและเงินได้พนักงาน	ฝ่าย HR	- ฝ่าย HR - หน่วยงานต้นสังกัด	ฝ่าย HR	HRMS
4	ข้อมูลตรวจประวัติอาชญากรรม	ฝ่าย HR	- ฝ่าย HR หน่วยงานต้นสังกัด	ฝ่าย HR	
5	ข้อมูลการตรวจสุขภาพก่อนเริ่มงาน	ฝ่าย HR	- ฝ่าย HR หน่วยงานต้นสังกัด	ฝ่าย HR	
	ข้อมูลกรรมการ/ผู้ถือหุ้น				
6	ข้อมูลผู้ถือหุ้น และข้อมูลการซื้อขายหุ้นของ Strategic Shareholders	ส่วนนักลงทุนสัมพันธ์	ส่วนนักลงทุนสัมพันธ์	ส่วนนักลงทุนสัมพันธ์	PDF
7	ข้อมูลการปิดสมุดทะเบียนผู้ถือหุ้น	ส่วนนักลงทุนสัมพันธ์	-ส่วนนักลงทุนสัมพันธ์ - สำนักเลขานุการบริษัท	ส่วนนักลงทุนสัมพันธ์	PDF
	ข้อมูลธุรกิจ				
8	กลยุทธ์องค์กร 1 ปี และ 5 ปี	หน่วยงานต้นสังกัด	- หน่วยงานต้นสังกัด - ผู้บริหารระดับสูง	หน่วยงานต้นสังกัด	Excel
9	สัญญาร่วมทุน	ส่วนกฎหมาย	- ส่วนกฎหมาย - ส่วนนักลงทุนสัมพันธ์	- สำนักเลขาฯ ส่วนนักลงทุนสัมพันธ์	Work Flow, Hard Copy
10	สัญญากู้ยืมเงินทุกประเภท	ส่วนกฎหมาย	- ส่วนกฎหมาย - หน่วยงานผู้ขอใช้บริการ	- ส่วนการเงิน	ECM
11	M.O.U. ในการร่วมดำเนินธุรกิจ	ส่วนกฎหมาย	- ฝ่ายกฎหมาย ส่วนนักลงทุนสัมพันธ์	- สำนักเลขาฯ - ส่วนนักลงทุนสัมพันธ์	ECM
12	ข้อมูล ข้อเท็จจริง และข้อสรุปต่างๆ ที่ได้จากการเจรจาหรือการดำเนินงานทางด้านกฎหมายทุกเรื่องที่ยังไม่ได้ถูกเปิดเผยต่อสาธารณะชน	ส่วนกฎหมาย	ส่วนกฎหมาย	ส่วนกฎหมาย	PDF
13	นโยบาย หรือคำสั่งขององค์กร หรือผู้บังคับบัญชาทุกประเภทที่กำหนดให้เป็นข้อมูลความลับ และห้ามเปิดเผย	ส่วนกฎหมาย	ส่วนกฎหมาย	ส่วนกฎหมาย	PDF
14	ข้อมูลอื่นๆ ที่เกี่ยวข้องกับการบริหารการดำเนินธุรกิจของบริษัท ที่ยังไม่ถึงเวลาประกาศใช้ หรือยังไม่ถึงเวลาเปิดเผยข้อมูลต่อสาธารณชน	สำนักเลขานุการบริษัท	สำนักเลขานุการบริษัท	สำนักเลขานุการบริษัท	
15	ใบเปรียบเทียบราคาน้ำก๊าซ และการขนส่งทางเรือ	ส่วนวางแผนและจัดหาก๊าซ	- ส่วนวางแผนและจัดหาก๊าซ	ส่วนวางแผนและจัดหาก๊าซ	Excel
16	ใบเสนอราคา น้ำก๊าซ และการขนส่งทางเรือ	ส่วนวางแผนและจัดหาก๊าซ	- ส่วนวางแผนและจัดหาก๊าซ	ส่วนวางแผนและจัดหาก๊าซ	PDF

No.	ประเภท/ ลักษณะข้อมูล	หน่วยงานผู้จัดทำข้อมูล	หน่วยงานผู้ใช้ข้อมูล (Data User)	หน่วยงานเจ้าของข้อมูล (Data Owner)	เก็บในระบบ
17	ใบเสนอราคาค่าขนส่ง	ส่วนขนส่งการวางแผนจัดส่งก๊าซ Bulk	- ส่วนขนส่งการวางแผนจัดส่งก๊าซ Bulk	ส่วนขนส่งการวางแผนจัดส่งก๊าซ Bulk	PDF
18	สัญญาในงานจัดจ้างงานขนส่ง	ส่วนกฎหมาย	- ส่วนจัดซื้อ - ส่วนขนส่งการวางแผนจัดส่งก๊าซ Bulk	ส่วนขนส่งการวางแผนจัดส่งก๊าซ Bulk	WorkFlow
19	สัญญาในงานจัดซื้อจัดจ้าง (น้ำก๊าซและการขนส่งทางเรือ)	ส่วนวางแผนและจัดหาก๊าซ	- ส่วนวางแผนและจัดหาก๊าซ	ส่วนวางแผนและจัดหาก๊าซ	PDF
20	สัญญาซื้อขายน้ำมันจากโรงกลั่น	ส่วนกฎหมาย	- ส่วนกฎหมาย -หน่วยงานเกี่ยวข้อง	ส่วนกฎหมาย, หน่วยงานที่เกี่ยวข้อง	ECM
	ข้อมูลตัวเลขทางการเงิน				
21	ยอดขายกำไรบาทต่อลิตร	OLP, BI	- ผู้บริหาร - OLP - ส่วนบัญชี	OLP	Max Station/SAP/Power BI
22	งบการเงินภายในสำหรับหน่วยงานต่างๆ	ส่วนบัญชี	- ส่วนบัญชี - หน่วยงานเกี่ยวข้อง	ส่วนบัญชี	PDF
23	ร่างงบการเงินสำหรับงวดไตรมาส หรือรายปี	ส่วนบัญชี	- ส่วนบัญชี - หน่วยงานเกี่ยวข้อง	ส่วนบัญชี	PDF
24	รายงานกำไรขั้นต้น ตัวเลขทางการเงิน (เช่น อัตราส่วนทางการเงิน งบประมาณ ปริมาณการขายสินค้า วิเคราะห์การเปลี่ยนแปลงระหว่างเดือน เป็นต้น)	ส่วนบัญชี	- ส่วนบัญชี - หน่วยงานเกี่ยวข้อง	ส่วนบัญชี	PDF
	ข้อมูลเกี่ยวกับระบบ				
25	รหัส Admin สำหรับเข้าระบบงาน	ส่วน IT	ส่วน IT	ส่วน IT	Excel
	ข้อมูลเกี่ยวกับการทำงาน/กระบวนการทำงาน				
26	ผลการประเมินคณะกรรมการรายคณะและรายบุคคล	สำนักเลขานุการบริษัท	คณะกรรมการบริษัท	สำนักเลขานุการบริษัท	PDF
27	ข้อมูลส่วนบุคคลที่เกี่ยวกับการจ้างงาน	ฝ่าย HR	ฝ่าย HR	ฝ่าย HR	Hard copy
28	ข้อมูลการจ่ายค่าตอบแทนและการปรับเงินประจำปีและการจ่ายโบนัส	ฝ่าย HR	ฝ่าย HR	ฝ่าย HR	Hard copy, Excel
29	ข้อมูลส่วนบุคคลของพนักงาน(แฟ้มประวัติ) ทั้งรายวัน และรายเดือน	ฝ่าย HR	ฝ่าย HR	ฝ่าย HR	

ข้อมูลลับ

No.	ประเภท/ ลักษณะข้อมูล	หน่วยงานผู้จัดทำข้อมูล	หน่วยงานผู้ใช้ข้อมูล (Data User)	หน่วยงานเจ้าของข้อมูล (Data Owner)	เก็บในระบบ
	ข้อมูลลูกค้า				
1	ข้อมูลลูกค้าโครงการ Taxi Transform/Auto Transform	ส่วนสนับสนุนงานสถานี	สนับสนุนสถานี, BI	ส่วนสนับสนุนงานสถานี	Google Sheet
2	ข้อมูลลูกค้าช่องทางการขายปลีกและขายส่ง	ฝ่ายขายร้าน Gas Shop / ส่วนการขาย	ฝ่ายขายร้าน Gas Shop / ส่วนการขาย	ฝ่ายขายร้าน Gas Shop / ส่วนการขาย	SAP /LMS/ Excel/PDF
3	เอกสารประกอบการอนุมัติวงเงินลูกค้า	ฝ่ายขายร้าน Gas Shop / ส่วนการขาย	ส่วนการเงิน	ส่วนการเงิน	PDF
	ข้อมูลผู้บริหาร/พนักงาน				
4	หนังสือเตือนพนักงาน	ฝ่าย HR	ฝ่าย HR	ฝ่าย HR	PDF
5	หนังสือให้ความยินยอมหักค่าจ้างและเงินได้อื่น	ฝ่าย HR	ฝ่าย HR	ฝ่าย HR	PDF
6	หนังสือเตือนด้วยวาจา(บันทึกเป็นหนังสือ)	ฝ่าย HR	ฝ่าย HR	ฝ่าย HR	PDF
7	หนังสือเลิกจ้าง	ฝ่าย HR	ฝ่าย HR	ฝ่าย HR	PDF
8	บันทึกแนบท้ายจ่ายเงินชดเชยเลิกจ้าง	ฝ่าย HR	ฝ่าย HR	ฝ่าย HR	PDF
9	ข้อมูลการตรวจสุขภาพประจำปี	ฝ่าย HR	ฝ่าย HR	ฝ่าย HR	Hard copy
10	ทะเบียนคุมเบอร์โทรศัพท์มือถือพนักงาน	ฝ่าย HR	ฝ่าย HR	ฝ่าย HR	Excel
	ข้อมูลกรรมการ/ผู้ถือหุ้น				
11	เอกสารส่วนบุคคลของกรรมการบริษัทและผู้บริหารระดับสูง	สำนักเลขานุการบริษัท	สำนักเลขานุการบริษัท	สำนักเลขานุการบริษัท	PDF
	ข้อมูลตัวเลขทางการเงิน				
12	งบประมาณการลงทุน (Plan / Monthly Registered)	หน่วยงานต้นสังกัด	- หน่วยงานต้นสังกัด - ส่วนงบประมาณ	หน่วยงานต้นสังกัด	Excel
13	งบประมาณประจำปี	หน่วยงานต้นสังกัด	- หน่วยงานต้นสังกัด - ส่วนงบประมาณ	หน่วยงานต้นสังกัด	Excel
14	ข้อมูลตัวเลขอื่นๆ เช่น แนวโน้มผลประกอบการ การวิเคราะห์งบการเงิน	ส่วนนักลงทุนสัมพันธ์	ส่วนนักลงทุนสัมพันธ์	ส่วนนักลงทุนสัมพันธ์	Excel
15	ข้อมูลที่เกี่ยวข้องกับการดำเนินธุรกิจตามโครงการพิเศษทุกประเภทที่ยังไม่ได้ถูกเปิดเผยต่อสาธารณะชน	ส่วนนักลงทุนสัมพันธ์	ส่วนนักลงทุนสัมพันธ์	ส่วนนักลงทุนสัมพันธ์	Excel
16	ข้อมูลยอดขาย Gas LPG	ส่วนการขาย, OLP, BI	- ผู้บริหาร - ส่วนการขาย - ส่วนบัญชี - ฝ่าย Supply Chain - OLP	ส่วนการขาย	SAP/ Power BI
17	ข้อมูลยอดขาย Gas ถัง และอุปกรณ์	ฝ่ายขายร้าน Gas Shop, ส่วนการขาย, BI	- ผู้บริหาร - ฝ่ายขายร้าน Gas Shop	- ฝ่ายขายร้าน Gas Shop, ส่วนการขาย	LMS/ Power BI

No.	ประเภท/ ลักษณะข้อมูล	หน่วยงาน ผู้จัดทำข้อมูล	หน่วยงาน ผู้ใช้ข้อมูล (Data User)	หน่วยงาน เจ้าของข้อมูล (Data Owner)	เก็บในระบบ
			- ส่วนการขาย - ฝ่ายโรงบรรจุก๊าซ - ส่วนบัญชี		
18	ข้อมูลยอดขายน้ำมัน	OLP, BI	- ผู้บริหาร - OLP - ส่วนบัญชี	- OLP	Max Station/SAP/Power BI
19	ยอดขายสถานี	OLP, BI	- ผู้บริหาร - OLP - ส่วนบัญชี	- OLP	Max Station/SAP/Power BI
20	ข้อมูลยอดขายน้ำมันและ LPG ของสมาชิก	OLP, BI	- ผู้บริหาร - OLP - ส่วนบัญชี	- OLP	CRM
21	ข้อมูลยอดขายแก๊สถังและอุปกรณ์เสริม ของสมาชิก	ฝ่ายขายร้าน Gas Shop, BI	- ผู้บริหาร - ฝ่ายขายร้าน Gas Shop - ส่วนบัญชี	- ฝ่ายขายร้าน Gas Shop	CRM
22	เป้าการขาย	ส่วนการขาย, ฝ่ายขายร้าน Gas Shop, OLP	- ผู้บริหาร - ฝ่ายขายร้าน Gas Shop - ส่วนบัญชี - โรงบรรจุก๊าซ	- ส่วนการขาย, ฝ่ายขายร้าน Gas Shop, OLP	Excel
	ข้อมูลธุรกิจ				
23	ข้อมูลโปรโมชั่น แคมเปญการตลาด	ส่วนการตลาด	ส่วนการตลาด	ส่วนการตลาด	Excel
24	ข้อมูลค่าการตลาด (GP/ต้นทุน)	ส่วนการตลาด	ส่วนการตลาด	ส่วนการตลาด	Excel
25	เอกสารอนุมัติราคาขายแก๊สหุงต้ม	ส่วนการตลาด	- ฝ่ายขายร้าน Gas Shop - ส่วนการขาย	ส่วนการตลาด	PDF
26	ข้อมูลธุรกิจใหม่ของบริษัท	ส่วนนักลงทุนสัมพันธ์	ส่วนนักลงทุนสัมพันธ์	ส่วนนักลงทุนสัมพันธ์	PDF
27	ข้อมูลการวิเคราะห์เปรียบเทียบผลการดำเนินงานของบริษัทเทียบกับคู่แข่ง	ส่วนนักลงทุนสัมพันธ์	ส่วนนักลงทุนสัมพันธ์	ส่วนนักลงทุนสัมพันธ์	Excel
28	ข้อมูลสารสนเทศก่อนการเปิดเผยข้อมูลต่อสาธารณะชน	ส่วนนักลงทุนสัมพันธ์	ส่วนนักลงทุนสัมพันธ์	ส่วนนักลงทุนสัมพันธ์	PDF
29	แผนการจัดซื้อก๊าซ	ส่วนวางแผนและจัดหาก๊าซ	ส่วนวางแผนและจัดหาก๊าซ	ส่วนวางแผนและจัดหาก๊าซ	Excel
30	แผนปรับปรุงสถานี	OLP	- OLP - ฝ่ายจัดซื้อ	OLP	Excel
31	แผนเปิดสถานี/สาขาใหม่	OLP, ฝ่ายขายร้าน Gas Shop	- OLP, - ฝ่ายขายร้าน Gas Shop	OLP, ฝ่ายขายร้าน Gas Shop	Excel
32	สัญญาเช่า / ร่างสัญญาเช่า	ส่วนกฎหมาย	- OLP - ส่วนกฎหมาย - ฝ่ายบัญชีและการเงิน	ส่วนกฎหมาย	ECM
33	สำนวนคดีความทุกประเภท	ส่วนกฎหมาย	ส่วนกฎหมาย	ส่วนกฎหมาย	Hard Copy
34	พยานหลักฐานในคดีทุกประเภท	ส่วนกฎหมาย	ส่วนกฎหมาย	ส่วนกฎหมาย	Hard Copy
35	แผนงานสืบทรัพย์และบังคับคดี	ส่วนกฎหมาย	ส่วนกฎหมาย	ส่วนกฎหมาย	Hard Copy

แนวปฏิบัติการกำหนดลำดับชั้นความลับของข้อมูล

No.	ประเภท/ ลักษณะข้อมูล	หน่วยงาน ผู้จัดทำข้อมูล	หน่วยงาน ผู้ใช้ข้อมูล (Data User)	หน่วยงาน เจ้าของข้อมูล (Data Owner)	เก็บในระบบ
36	นโยบายและแผนดำเนินงานภายในของส่วนกฎหมาย	ส่วนกฎหมาย	ส่วนกฎหมาย	ส่วนกฎหมาย	PDF
37	ผลการดำเนินงานบริษัท รายเดือน (แยกตามส่วนงาน)	หน่วยงานต้นสังกัด	สำนักเลานุการบริษัท	หน่วยงานต้นสังกัด	PDF
38	สัญญารักษาข้อมูลความลับ	ส่วนกฎหมาย	- ส่วนกฎหมาย - หน่วยงานผู้ขอใช้บริการ	ส่วนกฎหมาย	ECM
39	ข้อมูลที่เกี่ยวกับการดำเนินธุรกิจปกติทุกประเภทประเภทที่ยังไม่ได้เปิดเผยต่อสาธารณะชน	- ฝ่ายกฎหมาย - หน่วยงานเกี่ยวข้อง	- ฝ่ายกฎหมาย - หน่วยงานเกี่ยวข้อง	หน่วยงานต่นสังกัด	
40	ข้อมูลสัญญายืมถังของลูกค้า	ฝ่ายขายร้าน Gas Shop, ส่วนการขาย	ฝ่ายขายร้าน Gas Shop, ส่วนการขาย	ฝ่ายขายร้าน Gas Shop, ส่วนการขาย	Hard Copy/PDF
41	ข้อมูลโปรโมชั่น	ฝ่ายขายร้าน Gas Shop, ส่วนการขาย, ส่วนสนับสนุนงานสถานี	- ส่วนการขาย - ฝ่ายขายร้าน Gas Shop - ส่วนสนับสนุนงานสถานี	ส่วนการตลาด	PDF/Excel
42	ยอดสมาชิก Max card	ส่วนการตลาด	ส่วนการตลาด	ส่วนการตลาด	CRM
43	ข้อมูลบัตรสมาชิก Maxcard	ส่วนการตลาด	ส่วนการตลาด	ส่วนการตลาด	CRM
44	ยอด Active สมาชิก	ส่วนการตลาด	ส่วนการตลาด	ส่วนการตลาด	CRM
45	Incentive / Commission scheme	ฝ่ายการขายร้าน Gas Shop, ส่วนการขาย, ส่วนสนับสนุนงานสถานี	- ส่วนการขาย - ฝ่ายการขายร้าน Gas Shop - ส่วนสนับสนุนงานสถานี - ส่วนบัญชี - ฝ่ายบริหารทรัพยากรบุคคล	ฝ่ายการขายร้าน Gas Shop, ส่วนการขาย, ส่วนสนับสนุนงานสถานี	Excel
46	แบบก่อสร้างสถานีบริการ และราคาประเมิน	ส่วนวิศวกรรม	ส่วนวิศวกรรม	ส่วนวิศวกรรม	Excel
47	ข้อมูลชื่อที่อยู่สถานีบริการ Gas Shop และพิกัด	OLP, ฝ่ายขายร่าน Gas Shop	ทุกหน่วยงานที่ขอใช้ข้อมูล	OLP, ฝ่ายขายร่าน Gas Shop	Google Sheet
48	ข้อมูลน้ำมันและแก๊สสูญหาย (สถานี)	OLP	OLP	OLP	Excel
49	ข้อมูลแก๊ส Gain Loss (โรงบรรจุก๊าซ)	ฝ่ายโรงบรรจุก๊าซ	- ฝ่ายโรงบรรจุก๊าซ - ส่วนบัญชี	ฝ่ายโรงบรรจุก๊าซ	Excel
50	ปริมาณสินค้าคงเหลือ (น้ำก๊าซ)	ส่วนวางแผนและจัดหาก๊าซ	- ส่วนวางแผนและจัดหาก๊าซ - ส่วนบัญชี	ส่วนวางแผนและจัดหาก๊าซ	SAP
51	ปริมาณสินค้าคงเหลือ (แก๊สถัง)	ฝ่ายโรงบรรจุก๊าซ	- ฝ่ายโรงบรรจุก๊าซ - ส่วนบัญชี	ฝ่ายโรงบรรจุก๊าซ	LMS
52	ข้อมูลเกี่ยวกับการบริหารจัดการพื้นที่และค่าเช่า	BI	OLP	OLP	Site Management
53	ข้อมูลยอดแจกน้ำ โปรโมชั่น	OLP	OLP	OLP	Power BI
54	ข้อมูลทรัพย์สินในสถานีบริการ	OLP	OLP	OLP	AMS
55	ข้อมูลแผนการขยายสาขา และปรับปรุงสาขา	OLP, ฝ่ายขายร้าน Gas Shop	- OLP - ฝ่ายขายร้าน Gas Shop	OLP, ฝ่ายขายร้าน Gas Shop	
56	KPI (Functional KPI / KPI Cascade)	หน่วยงานต้นสังกัด	หน่วยงานต้นสังกัด	หน่วยงานต้นสังกัด	Excel
57	Corporate KPI	หน่วยงานต้นสังกัด	หน่วยงานต้นสังกัด	หน่วยงานต้นสังกัด	Excel

แนวปฏิบัติการกำหนดลำดับชั้นความลับของข้อมูล

No.	ประเภท/ ลักษณะข้อมูล	หน่วยงาน ผู้จัดทำข้อมูล	หน่วยงาน ผู้ใช้ข้อมูล (Data User)	หน่วยงาน เจ้าของข้อมูล (Data Owner)	เก็บในระบบ
58	Succession Planning	คณะกรรมการบริหาร	คณะกรรมการบริหาร	คณะกรรมการบริหาร	
59	อัตราดอกเบี้ย/ค่าธรรมเนียมที่มีภาระผูกพันกับธนาคาร (แบบเฉพาะราย)	ส่วนการเงิน	ส่วนบัญชี, ส่วนการเงิน	ส่วนการเงิน	
60	รายงานเคลื่อนไหวทางการเงิน (statement)	ส่วนการเงิน	ส่วนบัญชี, ส่วนการเงิน	ส่วนการเงิน	
61	สัญญาเช่าสถานีบริการทุกประเภท	ส่วนกฎหมาย	- ส่วนกฎหมาย - OLP	ส่วนกฎหมาย	ECM
62	สัญญาเช่าพื้นที่โรงบรรจุก๊าซ	ส่วนกฎหมาย	- ส่วนกฎหมาย - ฝ่ายโรงบรรจุก๊าซ	ฝ่ายโรงบรรจุก๊าซ	ECM
63	สัญญาเช่าพื้นที่จัดเก็บถังแก๊สเปล่า	ส่วนกฎหมาย	- ส่วนกฎหมาย - ฝ่ายโรงบรรจุก๊าซ	ฝ่ายโรงบรรจุก๊าซ	ECM
64	สัญญาแต่งตั้งตัวแทนจำหน่าย	ส่วนกฎหมาย	ฝ่ายกฎหมาย หน่วยงานผู้ขอใช้บริการ	ส่วนการขาย	ECM
65	สัญญาซื้อขายทรัพย์สินทุกประเภท	ส่วนกฎหมาย	ฝ่ายกฎหมาย หน่วยงานผู้ขอใช้บริการ	ส่วนกฎหมาย	ECM
66	สัญญาว่าจ้างทุกประเภท	ส่วนกฎหมาย	- ฝ่ายกฎหมาย - หน่วยงานผู้ขอใช้บริการ - ฝ่ายจัดซื้อ	ฝ่ายจัดซื้อ	ECM
67	ข้อมูลสัญญากับคู่ค้า และ ลูกค้าโครงการ Taxi Transform/Auto Transform	OLP	OLP	OLP	PDF, Hard Copy
68	ข้อมูลสมาชิกโครงการ Taxi Transform	OLP, BI	OLP	OLP	Google Sheet
69	ข้อมูลสมาชิกโครงการ Taxi Advertising	OLP, BI	OLP	OLP	CRM
70	ข้อมูลสมาชิกโครงการ Auto Transform	OLP, BI	OLP	OLP	CRM
71	สัญญา บันทึกข้อตกลง และเอกสารอื่นใดที่เกี่ยวข้องกับการดำเนินธุรกิจ และการปฏิบัติตามกฎหมายทุกประเภท	ส่วนกฎหมาย	- ส่วนกฎหมาย - หน่วยงานผู้ขอใช้บริการ	ส่วนกฎหมาย	ECM
72	เอกสารสิทธิทุกประเภท	ส่วนกฎหมาย, คู่สัญญา, ราชการ	- ส่วนกฎหมาย - หน่วยงานผู้ขอใช้บริการ	ส่วนกฎหมาย	Hard Copy
73	กรมธรรม์ประกันภัยของสาขา	OLP	OLP	OLP	PDF
74	กำลังการผลิต(capacity)	ฝ่ายโรงบรรจุก๊าซ	ฝ่ายโรงบรรจุก๊าซ	ฝ่ายโรงบรรจุก๊าซ	Excel
	ข้อมูลเกี่ยวกับระบบ				
75	รหัสผ่านสำหรับเข้าระบบของสถาบันการเงิน	ส่วนการเงิน	ส่วนการเงิน	ส่วนการเงิน	
76	System/net work diagram	ส่วน IT	ส่วน IT	ส่วน IT	PDF
	ข้อมูลเกี่ยวกับการทำงาน/กระบวนการทำงาน				
77	รายงานสรุปผลการตรวจสอบ	ส่วนตรวจสอบภายใน	-ส่วนงานที่เกี่ยวข้อง -ส่วนตรวจสอบภายใน	ส่วนตรวจสอบภายใน	Team Central/ PDF

แนวปฏิบัติการกำหนดลำดับชั้นความลับของข้อมูล

No.	ประเภท/ ลักษณะข้อมูล	หน่วยงาน ผู้จัดทำข้อมูล	หน่วยงาน ผู้ใช้ข้อมูล (Data User)	หน่วยงาน เจ้าของข้อมูล (Data Owner)	เก็บในระบบ
78	รายงานการประชุมคณะกรรมการตรวจสอบ	ส่วนตรวจสอบภายใน	- ส่วนงานที่เกี่ยวข้อง - ส่วนตรวจสอบภายใน	ส่วนตรวจสอบภายใน	PDF
79	กระดาษทำการ	ส่วนตรวจสอบภายใน	- ส่วนงานที่เกี่ยวข้อง - ส่วนตรวจสอบภายใน	ส่วนตรวจสอบภายใน	Team Central
80	รายงานการประชุมคณะกรรรมการบริษัท	สำนักเลขานุการบริษัท	คณะกรรมการบริษัท	สำนักเลขานุการบริษัท	PDF
81	Significant contracts	ส่วนกฎหมาย	สำนักเลขานุการบริษัท	สำนักเลขานุการบริษัท	ECM
82	ใบเสนอราคาขาย	ส่วนการขาย	ส่วนการขาย	ส่วนการขาย	PDF
83	บันทึกการสอบสวนข้อเท็จจริง	ส่วนกฎหมาย, HR, BU ที่เกี่ยวข้อง	- ส่วนกฎหมาย - HR - หน่วยงานที่ขอใช้ข้อมูล	- ส่วนกฎหมาย - HR - หน่วยงานที่ขอใช้ข้อมูล	
84	ใบสั่งซื้อ	- ฝ่ายจัดซื้อ	- ฝ่ายจัดซื้อ - หน่วยงานต้นสังกัด	ฝ่ายจัดซื้อ	VRM
85	ใบสั่งซื้อ น้ำก๊าซ และการขนส่งทางเรือ	ส่วนวางแผนและจัดหาก๊าซ	ส่วนวางแผนและจัดหาก๊าซ	ส่วนวางแผนและจัดหาก๊าซ	PDF
86	ใบเปรียบเทียบราคา	ฝ่ายจัดซื้อ	- ฝ่ายจัดซื้อ - หน่วยงานต้นสังกัด	ฝ่ายจัดซื้อ	VRM
87	ข้อมูลประเมินผลการปฏิบัติงานประจำปี	ฝ่าย HR	ฝ่าย HR	ฝ่าย HR	PMS
88	ใบเสนอราคา	ฝ่ายจัดซื้อ	- ฝ่ายจัดซื้อ - หน่วยงานต้นสังกัด	ฝ่ายจัดซื้อ	VRM
89	ใบสรุปผลการประกวดราคา	ฝ่ายจัดซื้อ	- ฝ่ายจัดซื้อ - หน่วยงานต้นสังกัด	ฝ่ายจัดซื้อ	PDF
90	สัญญาในงานจัดซื้อจัดจ้าง	ฝ่ายจัดซื้อ	- ฝ่ายจัดซื้อ - หน่วยงานต้นสังกัด	ฝ่ายจัดซื้อ	ECM
91	ข้อมูลสัญญาเช่าห้องพักพนักงาน	OLP	OLP	OLP	PDF
92	ข้อมูลเรียกร้องการเคลมประกันภัยสถานี	OLP	OLP	OLP	PDF, Excel
93	ข้อมูลจากเอกสารหนังสือผู้รับมอบอำนาจ	OLP	OLP	OLP	Hard Copy, PDF
94	เอกสารใบรับผลประโยชน์ (กรณีประกันชีวิต)	ฝ่าย HR	ฝ่าย HR	ฝ่าย HR	Hard Copy

ตัวอย่างทะเบียนคุมเอกสารลับ

ลำดับ	เลขที่เอกสาร	ชื่อเอกสาร	การจัดเก็บ	หมายเหตุ

ตัวอย่างทะเบียนการยืม-คืนเอกสารลับ

ลำดับ	เลขที่เอกสาร	ชื่อเอกสาร	วัน/เดือน/ปีที่ยืมเอกสาร	กำหนดการคืนเอกสาร	วัน/เดือน/ปีที่ส่งคืนเอกสาร	ชื่อ-สกุลผู้ยืมเอกสาร	หน่วยงาน	ลงนามผู้รับ/คืนเอกสาร	ผู้ตรวจสอบการรับ/คืน *(หน่วยงานเจ้าของเอกสาร)*