



นโยบายการคุ้มครองข้อมูลส่วนบุคคล

1. หลักการทั่วไป (General Principle)

1.1 ความทั่วไป

บริษัท ไชโน โลจิสติกส์ คอร์ปอเรชั่น จำกัด (มหาชน) (“บริษัท”) และบริษัทย่อย ยึดมั่นในการดำเนินธุรกิจที่สอดคล้องตามบทบัญญัติของกฎหมายที่เกี่ยวข้อง โดยเฉพาะอย่างยิ่งการให้ความสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของผู้มีส่วนได้เสียกับการดำเนินธุรกิจของบริษัท บริษัทได้พัฒนาระบบการบริหารจัดการข้อมูลส่วนบุคคลด้วยระบบปฏิบัติงาน และระบบเทคโนโลยีสารสนเทศที่ทันสมัย และมีความมั่นคงปลอดภัยต่อการคุ้มครองความเป็นส่วนตัวของข้อมูลส่วนบุคคลที่มีประสิทธิภาพ โดยกำหนดให้เฉพาะเจ้าหน้าที่ของบริษัท หรือบุคคลที่เกี่ยวข้องเท่านั้นที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคล นอกจากนี้ บริษัทยังจัดให้มีระบบการตรวจสอบการเข้าถึงและการใช้ข้อมูลส่วนบุคคลอย่างเคร่งครัด ตลอดจนจัดให้มีการปรับปรุงและพัฒนาาระบบการจัดเก็บและรักษาข้อมูลส่วนบุคคลอย่างสม่ำเสมอเพื่อให้ระบบมีการจัดเก็บข้อมูลส่วนบุคคลที่ถูกต้องเชื่อถือได้ และเพื่อป้องกันไม่ให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล การแก้ไขส่วนบุคคลโดยผู้ไม่มีหน้าที่เกี่ยวข้อง หรือการนำข้อมูลส่วนบุคคลไปใช้นอกเหนือจากวัตถุประสงค์ที่บริษัทได้แจ้งให้ผู้มีส่วนได้เสียได้ทราบไว้แต่แรก

นโยบายฉบับนี้ได้อธิบายถึงประเภทของข้อมูลส่วนบุคคล และวัตถุประสงค์ของการเก็บรวบรวมเพื่อนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย ระยะเวลาในการเก็บรวบรวมข้อมูล ประเภทของบุคคล หรือหน่วยงานซึ่งบริษัทอาจเปิดเผยข้อมูลส่วนบุคคลที่บริษัทรวบรวมไว้ สิทธิของเจ้าของข้อมูลส่วนบุคคล รวมถึงมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่สอดคล้องกับบทบัญญัติของกฎหมาย ตลอดจนข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคลของบริษัท

นโยบายฉบับนี้ยังถือเป็นส่วนหนึ่งของข้อตกลงและเงื่อนไขการใช้งานบริการต่าง ๆ ของบริษัท บริษัทอาจแก้ไขปรับปรุง เพิ่มเติม เปลี่ยนแปลง นโยบายนี้โดยจะแจ้งให้เจ้าของข้อมูลทราบและขอความยินยอมจากเจ้าของข้อมูลตามที่กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลกำหนด

1.2 คำจำกัดความ

เพื่อให้เกิดความชัดเจนในการสื่อสารกับผู้มีส่วนได้เสียในการดำเนินธุรกิจ และไม่ให้เกิดข้อกังวลเกี่ยวกับการตีความของคำบางคำในเอกสารฉบับนี้ บริษัทจึงได้จัดทำคำจำกัดความไว้ ดังนี้

“บริษัท” หมายถึง บริษัท ไชโน โลจิสติกส์ คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทย่อย และให้หมายรวมถึงบุคคลคนเดียวหรือหลายคนที่ได้รับมอบหมายให้มีอำนาจกระทำการแทนบริษัท ไชโน โลจิสติกส์ คอร์ปอเรชั่น จำกัด (มหาชน) และบริษัทย่อย

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลที่เกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม

“ข้อมูลส่วนบุคคลที่มีความอ่อนไหว” หมายถึง ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความ

พิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

“บุคลากร” หมายถึง บุคลากรของบริษัท ซึ่งรวมถึง กรรมการบริษัท ผู้บริหาร พนักงาน และลูกจ้างทุกคนของบริษัท

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายถึง บุคคลหรือนิติบุคคล ซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายถึง บุคคลหรือนิติบุคคล ซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

2. หลักการรวบรวมข้อมูลอย่างจำกัด (Collection Limitation Principle)

2.1 ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม ใช้ หรือเปิดเผย

นโยบายฉบับนี้จะใช้กับข้อมูลส่วนบุคคลที่บริษัทอาจเก็บรวบรวม ใช้ หรือเปิดเผย รวมถึงกรณีที่เจ้าของข้อมูลได้ให้ความยินยอมไว้กับบริษัท ดังนี้

- (ก) ข้อมูลส่วนบุคคลทั่วไป เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด หมายเลขบัตรประจำตัวประชาชน ที่อยู่ตามบัตรประชาชน ที่อยู่ตามภูมิลำเนา ที่อยู่ปัจจุบัน หมายเลขโทรศัพท์ หมายเลขโทรศัพท์มือถือ สถานภาพทางครอบครัว บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ รูปถ่ายในบัตรประชาชน หมายเลขเลเซอร์ด้านหลังบัตรประชาชน
- (ข) ข้อมูลส่วนบุคคลที่มีความอ่อนไหว เช่น ข้อมูลเกี่ยวกับสุขภาพ ศาสนา หมู่เลือด ผลการตรวจสุขภาพ ประวัติการรักษาพยาบาล ผลการวินิจฉัยโรค ข้อมูลสุขภาพ ข้อมูลประวัติอาชญากรรม ภาพสแกนใบหน้า ดวงตา หรือลายนิ้วมือ
- (ค) ข้อมูลส่วนบุคคลอื่น ๆ เช่น ประวัติการทำงาน ทะเบียนรถยนต์ รถจักรยานยนต์ที่ได้จดทะเบียนไว้กับหน่วยงานราชการ หมายเลขอ้างอิงผลิตภัณฑ์ที่ใช้ผลิตภัณฑ์ได้ลงทะเบียนเพื่อรับประกันสินค้าหรือบริการนั้น ๆ สถานะทางการเงิน รายได้ ภาระหนี้ พฤติกรรมการบริโภค ตำแหน่งที่มีการใช้งานบริการของบริษัท และ/หรือความสนใจของเจ้าของข้อมูลเมื่อประกอบกับข้อมูลอื่นอันทำให้สามารถระบุตัวบุคคลผู้เป็นเจ้าของข้อมูลได้

2.2 การเก็บรวบรวม และการได้รับข้อมูลส่วนบุคคล

บริษัทยึดมั่นตามบทบัญญัติของกฎหมาย โดยจะเก็บรวบรวมข้อมูลส่วนบุคคลจากเจ้าของข้อมูลเท่านั้น เว้นแต่กรณีจำเป็นที่เจ้าของข้อมูลไม่อาจหรือไม่ได้เป็นผู้ที่เก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าวไว้ บริษัทอาจเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่น ทั้งนี้จะเป็นไปเฉพาะแต่กรณีที่บริษัทได้รับความยินยอมเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลส่วนบุคคลเท่านั้น โดยทั่วไปกรณีที่บริษัทอาจเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นได้แก่



2.2.1 ผู้สมัครงาน หรือพนักงาน

- (ก) ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับสุขภาพ หรือโรคประจำตัวของผู้สมัครงานที่บริษัทกำหนดให้ผู้ที่จะเข้าทำงานกับบริษัทในฐานะลูกจ้าง หรือพนักงานทำการตรวจสอบสุขภาพของตนเองก่อนเข้าทำงาน โดยให้สถานพยาบาลที่ทำการตรวจสุขภาพส่งผลการตรวจให้แก่บริษัท
- (ข) ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับประวัติการถูกดำเนินคดีทางกฎหมาย (ประวัติอาชญากรรม) โดยบริษัทกำหนดให้ผู้ที่จะเข้าทำงานทำการตรวจสอบประวัติอาชญากรรม หรือยินยอมให้บริษัทไปทำการตรวจประวัติอาชญากรรมแทนผู้สมัครงาน หรือพนักงาน
- (ค) ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับประวัติการทำงานก่อนหน้าที่จะทำงานกับบริษัท โดยบริษัทได้กำหนดให้เจ้าของข้อมูลส่วนบุคคลให้ความยินยอมโดยชัดแจ้งเป็นหนังสือแก่บริษัทก่อนทุกครั้ง โดยบริษัทจะแจ้งการให้ความยินยอมให้แก่บุคคลภายนอกนั้น ๆ ทราบล่วงหน้าก่อนการส่งข้อมูลดังกล่าวมายังบริษัท

2.2.2 ลูกค้า

ในกรณีที่เจ้าของข้อมูลส่วนบุคคลให้ความสนใจ หรือสั่งซื้อสินค้าจากบริษัท รวมถึงการติดต่อเพื่อบริการหลังการขายการติดต่อระหว่างเจ้าของข้อมูลกับบริษัทไม่ว่าจะเป็นทางโทรศัพท์ อีเมล แอปพลิเคชันของบริษัท แอปพลิเคชันที่ใช้ในการติดต่อสื่อสาร ศูนย์บริการลูกค้า หรือการติดต่อโดยวิธีการอื่นใด บริษัทอาจดำเนินการบันทึกข้อมูลการติดต่อสื่อสารเหล่านั้นเพื่อวัตถุประสงค์ต่าง ๆ เช่น เพื่อใช้เป็นหลักฐาน เพื่อพัฒนาและปรับปรุงบริการ เพื่อติดตามความพึงพอใจของเจ้าของข้อมูล เพื่ออบรมบุคลากร เพื่อประเมินผลงานบุคลากร เพื่อวิเคราะห์ข้อมูล รวมถึงเพื่อพัฒนาระบบของบริษัท

3. หลักการคุณภาพของข้อมูล (Data Quality Principle)

ก่อนหรือขณะที่บริษัททำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้มีส่วนได้เสีย บริษัทจะมีกระบวนการในการบริหารจัดการ วิเคราะห์ข้อมูลส่วนบุคคลต่าง ๆ ด้วยหลักการ

- ความถูกต้อง (Accuracy)
- ความสมบูรณ์ (Completeness)
- ความเที่ยง (Consistency)
- ความเป็นปัจจุบัน (Timeliness)
- ความเป็นเอกลักษณ์ (Uniqueness)
- ความแม่นยำ (Validity)

ทั้งนี้ บริษัทได้จัดผู้เกี่ยวข้องทำการวิเคราะห์ วางแผนเพื่อให้มีการเก็บรวบรวมข้อมูลเฉพาะที่มีความเป็นเอกลักษณ์ เที่ยงตรงที่เหมาะสมกับกระบวนการต่าง ๆ ข้างต้น เพื่อการนำไปใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้มีส่วนได้เสียให้เกิดประโยชน์สูงสุด การตรวจสอบถึงความถูกต้อง ความแม่นยำตรงของข้อมูลที่ได้รับก่อนที่จะมีการเก็บรวบรวม ไม่ว่าจะการบันทึกการข้อมูลเป็นหนังสือหรือระบบอิเล็กทรอนิกส์ เพื่อให้มีความครบถ้วนถูกต้อง รวมทั้งจัดให้มีการตรวจสอบความถูกต้องขอข้อมูลจากแหล่งข้อมูลที่เชื่อถือได้หรือตามที่กฎหมาย



กำหนดให้เป็นหน่วยงานที่มีอำนาจหน้าที่ในการจัดการเกี่ยวกับข้อมูลส่วนบุคคลนั้น ๆ รวมถึงการจัดการเพื่อการปกป้องข้อมูลส่วนบุคคล การรักษาความปลอดภัยและความมั่นคงของข้อมูล เพื่อเป็นป้องกันไม่ให้ข้อมูลรั่วหรือรั้งทั้งในเชิงกฎหมาย และเชิงพาณิชย์ในอนาคต

4. หลักการระบุวัตถุประสงค์ (Purpose Specification Principle)

บริษัทกำหนดวัตถุประสงค์อันจำเป็นเพื่อให้บรรลุวัตถุประสงค์ร่วมกันกับการให้บริการ สิทธิประโยชน์แก่เจ้าของข้อมูลส่วนบุคคล แยกตามประเภทของผู้มีส่วนได้เสียกับการดำเนินธุรกิจของบริษัท ดังนี้

4.1 ผู้ถือหุ้น

บริษัทจะเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของผู้ถือหุ้นเพื่อการลงนามผูกพันในสัญญาธุรกิจ สัญญาทั่วไป การอนุมัติการดำเนินการต่าง ๆ มอบอำนาจในการดำเนินการทางธุรกิจ กฎหมาย ธุรกรรมธนาคาร การติดต่อหน่วยงานราชการ การดำเนินการทั่วไปในการเชิญประชุม แจ้งผลของการประชุม การจัดการเงินปันผล รายงานผลการดำเนินการของบริษัทตามระเบียบหรือตามที่กฎหมายกำหนด

4.2 พนักงานและบุคคลในครอบครัว

บริษัทจะเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของพนักงานในขอบเขตของการสรรหา คัดเลือกเข้าทำงาน การทำสัญญาว่าจ้าง การยืนยันตัวตน การคำนวณและจ่ายค่าจ้าง ผลตอบแทน การประเมินผลการทำงาน การปรับค่าจ้าง การเก็บประวัติความประพฤติทางวินัยรวมถึงบทลงโทษ การฝึกอบรม และการบริหารงานบุคคลในฐานะที่พนักงานเป็นลูกจ้างตามสัญญาจ้างแรงงาน การตรวจสอบประวัติด้านอาชญากรรม การเลื่อน โยกย้ายตำแหน่งงาน การตรวจสอบสุขภาพทั้งตามที่กฎหมายกำหนดและที่บริษัทจัดให้ และรวมถึงการจัดสวัสดิการ ผลตอบแทน สิทธิประโยชน์ให้แก่พนักงานและครอบครัวของพนักงาน และการส่งข้อมูลให้แก่หน่วยงานภายนอกอันเป็นการปฏิบัติตามกฎหมายที่เกี่ยวข้องกับสรรพากร ประกันสังคม การพัฒนาฝีมือแรงงาน กรมบังคับคดี และการบริหารสำนักงาน การติดต่อประสานงานภายใน การเบิกค่าใช้จ่าย การถือครองทรัพย์สิน การจัดการด้านธุรการอาคารสถานที่ การจัดการจดหมายและไปรษณีย์ การบันทึกการเข้า-ออกพื้นที่ทำงาน การตรวจสอบ ตรวจสอบประเมินทั้งจากหน่วยงานภายในและภายนอก

4.3 คู่ค้า

บริษัทจะเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของคู่ค้า ซึ่งครอบคลุมไปถึงเจ้าของผลิตภัณฑ์ผู้ฝากขาย (Brand) ตัวแทนจำหน่าย ผู้ว่าจ้าง รวมถึงบุคคลที่ต้องดำเนินการตามคำสั่ง การมอบหมายของคู่ค้า ในขอบเขตของการเปิดบัญชีลูกหนี้การค้ารายใหม่ การเสนอราคา การเจรจาต่อรอง การจัดกิจกรรมส่งเสริมการขาย เปิดตัวสินค้า สาธิตสินค้า การบริหารจัดการด้านการขาย การโฆษณา การจ่ายรางวัลตอบแทนการขาย และการขึ้นทะเบียนผู้ขาย การจัดซื้อจัดจ้าง การประเมินผู้ขาย การเปิดบัญชีเจ้าหนี้การค้า การว่าจ้างสัญญาบริการต่าง ๆ กรณีที่เป็นวิทยากรหรือผู้รับเชิญให้บรรยาย ให้คำแนะนำเกี่ยวกับกระบวนการฝึกอบรม การสัมมนา การประชุม เป็นประวัติส่วนตัว ทั้งการศึกษา ประสบการณ์การทำงาน ความสามารถพิเศษ ภาพถ่ายขณะดำเนินกิจกรรม กรณีเป็นผู้ตรวจสอบ ตรวจสอบประเมินจากหน่วยงานภายนอก บริษัทจะเก็บรวบรวมข้อมูลส่วนบุคคลของผู้ตรวจสอบ ตรวจสอบประเมินไว้เฉพาะเท่าที่ใช้ในการยืนยันตัวตนเท่านั้น



ลูกค้า

บริษัทจะเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของลูกค้า เพื่อประโยชน์ของลูกค้าตั้งแต่การบริการก่อน การขาย ขณะที่ทำการซื้อขาย และบริการหลังการขาย การรีวิว (การแสดงความคิดเห็น การประชาสัมพันธ์ การแสดงความรู้สึก การแจ้งผลลัพธ์ของการใช้สินค้าและ/หรือผลิตภัณฑ์) การสำรวจความพึงพอใจ การแลกเปลี่ยนสินค้า การจัดการข้อร้องเรียนลูกค้า การนำเสนอโปรโมชั่น การแจ้งสิทธิประโยชน์แก่ลูกค้า การสำรวจความพึงพอใจ การจัดการกิจกรรมระหว่างลูกค้ากับเจ้าของผลิตภัณฑ์ (Brand) ที่จัดการผ่านระบบ Live หรือ VDO conference ซึ่งจะมีการเก็บ รวบรวม ใช้ เปิดเผยข้อมูลของบุคคลผู้ที่เข้าร่วมกิจกรรมตามเงื่อนไขที่บริษัทหรือเจ้าของผลิตภัณฑ์กำหนด

5. หลักการใช้ข้อมูลอย่างจำกัด (Use Limitation Principle)

บริษัทจะพิจารณาอย่างรอบคอบในการใช้ข้อมูลส่วนบุคคลของผู้มีส่วนได้เสียอย่างจำกัดภายใต้ขอบเขตของวัตถุประสงค์ที่ได้แจ้งไว้กับผู้มีส่วนได้เสียเมื่อก่อนหรือขณะเก็บรวบรวมข้อมูลส่วนบุคคลนั้น ๆ

นอกเหนือจากการคำนึงถึงความเป็นส่วนตัวและสิทธิขั้นพื้นฐานของผู้มีส่วนได้เสียในฐานะเจ้าของข้อมูลส่วนบุคคล ประกอบกับบทบัญญัติ กฎ ระเบียบ ข้อบังคับ ข้อกำหนดของทางราชการที่เกี่ยวข้อง บริษัทจะพิจารณาใช้ข้อมูลส่วนบุคคลเพื่อประโยชน์หรือตอบสนองของผู้มีส่วนได้เสียในฐานะลูกค้า ผู้รับบริการ ภายใต้ขอบเขตแห่งวัตถุประสงค์อย่างจำกัด เพื่อการดังต่อไปนี้

- (ก) ติดต่อเพื่อตอบคำถามจากลูกค้า
- (ข) การส่งสินค้า บริการ หรือผลิตภัณฑ์ที่สั่งซื้อ
- (ค) การจัดการและการปฏิบัติตามสัญญา
- (ง) การให้การสนับสนุนและบำรุงรักษาผลิตภัณฑ์
- (จ) การวิจัยตลาดและการพัฒนาผลิตภัณฑ์และบริการใหม่
- (ฉ) การแนะนำข้อเสนอทางการตลาด การสื่อสารทางการตลาด
- (ช) การจัดหาและการสื่อสารข้อมูลการจัดหางานให้กับผู้สมัครงาน (รวมถึงนักศึกษาฝึกงาน) และการจัดการการสรรหาของบริษัท
- (ซ) วัตถุประสงค์อื่นที่เกี่ยวข้องกับข้อต่าง ๆ ข้างต้น หากต้องได้มาหรือใช้ข้อมูลส่วนบุคคลเพื่อวัตถุประสงค์อื่น นอกเหนือจากที่ได้ระบุไว้ข้างต้น จะต้องได้รับความยินยอมก่อนการได้มาหรือใช้ข้อมูลดังกล่าวตามความจำเป็น

6. หลักการรักษาความปลอดภัยของข้อมูล (Security Safeguards Principle)

บริษัทได้กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลโดยคำนึงถึงสิทธิขั้นพื้นฐานของข้อมูลส่วนบุคคลของผู้มีส่วนได้เสีย ด้วยการออกแบบระบบสารสนเทศและระบบเครือข่ายและคอมพิวเตอร์ให้มีความมั่นคงปลอดภัยอย่างเหมาะสมที่สุด เพื่อสนับสนุนการดำเนินงานของบริษัทได้อย่างต่อเนื่อง สอดคล้องกับบทบัญญัติของกฎหมายที่เกี่ยวข้อง รวมทั้งเป็นการป้องกันภัยคุกคามที่อาจก่อให้เกิดความเสียหายแก่บริษัท



- 6.1 บริษัทจัดให้มีหน้าที่ดูแลให้มีการกำหนดนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และบริษัทต้องทำการสื่อสารนโยบายดังกล่าวเพื่อสร้างความเข้าใจและสามารถปฏิบัติตามได้อย่างถูกต้อง โดยเฉพาะอย่างยิ่งระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานด้านอื่นภายในบริษัท เพื่อให้มีการประสานงานและสามารถดำเนินธุรกิจได้ตามเป้าหมายที่ตั้งไว้
- 6.2 บริษัทจัดให้มีการทบทวนนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 (หนึ่ง) ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท
- 6.3 บริษัทกำหนดผู้ที่มีหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศไว้เป็นการเฉพาะ เพื่อให้มั่นใจว่าบริษัทสามารถจัดหาวิธีการหรือแนวทางด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงหรือจัดการความเสี่ยงที่มีอยู่ แล้วนำเสนอให้กับผู้บริหารเพื่อพิจารณาในการจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ
- 6.4 บริษัทได้ระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเพื่อครอบคลุมความเสี่ยงสำคัญ เช่น
- (ก) ความเสี่ยงจากบุคลากร
 - (ข) ความเสี่ยงจาก Software และข้อมูล
 - (ค) ความเสี่ยงจากระบบเครือข่ายและอินเทอร์เน็ต
 - (ง) ความเสี่ยงจาก Hardware และอุปกรณ์คอมพิวเตอร์
 - (จ) ความเสี่ยงจากการเงิน
 - (ฉ) ความเสี่ยงจากอุทกภัย ภัยพิบัติ
 - (ช) ความเสี่ยงจากแผ่นดินไหว อาคารพังถล่ม
 - (ซ) ความเสี่ยงจากอัคคีภัย
 - (ฌ) ความเสี่ยงจากการโจรกรรม
 - (ญ) ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง
- 6.5 บริษัทกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่บริษัทยอมรับได้จัดทำตารางลักษณะรายละเอียดความเสี่ยง โดยมีหัวข้อเรื่อง ชื่อความเสี่ยง ประเภทความเสี่ยง ลักษณะความเสี่ยง ปัจจัยความเสี่ยง และผลกระทบ เป็นต้น กำหนดระดับโอกาสการเกิดเหตุการณ์และระดับความรุนแรงของผลกระทบความเสี่ยง รวมถึงการทำแผนภูมิความเสี่ยง
- 6.6 บริษัทกำหนดตัวชี้วัดระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์
- 6.7 บริษัทห้ามบุคลากรของบริษัทใช้เครือข่ายคอมพิวเตอร์ เพื่อกระทำการอันผิดกฎหมายและขัดต่อศีลธรรมอันดีของสังคม เช่น การจัดทำเว็บไซต์เพื่อดำเนินการค้าขาย หรือเผยแพร่สิ่งที่มีผิดกฎหมาย หรือขัดต่อศีลธรรมอันดี เป็นต้น



- 6.8 บริษัทไม่อนุญาตให้บุคลากรของบริษัทใช้เครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ด้วยชื่อบัญชีผู้ใช้ของผู้อื่น ทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาตจากเจ้าของชื่อบัญชีผู้ใช้
- 6.9 บริษัทห้ามบุคลากรของบริษัทเข้าใช้ระบบคอมพิวเตอร์และข้อมูลที่มีการป้องกันการเข้าถึงของผู้อื่น เพื่อแก้ไข ลบ เพิ่มเติม หรือคัดลอก
- 6.10 บริษัทห้ามบุคลากรของบริษัทเผยแพร่ข้อมูลของผู้อื่น หรือของหน่วยงาน โดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูลนั้น ๆ
- 6.11 ห้ามผู้ใดก่อวินาศกรรม ชัดขวาง หรือทำลายให้ทรัพยากรและเครือข่ายคอมพิวเตอร์ของบริษัทเกิดความเสียหาย เช่น การส่งไวรัสคอมพิวเตอร์ การบ่อนโปรแกรมที่ทำให้เครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายปฏิเสธการทำงาน เป็นต้น
- 6.12 ห้ามผู้ใดลักลอบดักจับข้อมูลในเครือข่ายคอมพิวเตอร์ของบริษัท และของผู้อื่นที่อยู่ระหว่างการรับและส่งในเครือข่ายคอมพิวเตอร์
- 6.13 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ หรือเปิดไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ต ผู้ใช้งานต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนทุกครั้ง
- 6.14 บริษัทมอบหมายหน้าที่ให้กับผู้ใช้งานในฝ่ายเทคโนโลยี รับผิดชอบการดูแลระบบสารสนเทศที่บริษัทใช้งานให้มีความมั่นคงปลอดภัยของระบบสารสนเทศ และควบคุมการปฏิบัติงาน เพื่อให้คงไว้ซึ่งนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของบริษัท
- 6.15 พนักงานของบริษัททุกคนต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของบริษัท ในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของบริษัท รวมทั้งจะต้องไม่กระทำการละเมิดต่อกฎหมายที่เกี่ยวข้องกับการกระทำผิดเกี่ยวกับคอมพิวเตอร์
- 6.16 บริษัทไม่อนุญาตให้ผู้ใช้งานติดตั้ง แก้ไข เปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของบริษัท เว้นแต่ได้รับคำปรึกษาหรือคำแนะนำจากผู้ดูแลระบบ หรือได้รับอนุญาตจากผู้มีอำนาจสูงสุดของหน่วยงาน
- 6.17 บริษัทกำหนดเส้นทางการเชื่อมต่อระบบเครือข่ายเพื่อการเข้าใช้งานระบบอินเทอร์เน็ต โดยต้องผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall หรือ Proxy โดยเครื่องคอมพิวเตอร์ของบริษัทก่อนทำการเชื่อมต่อระบบเครือข่าย ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการก่อน และภายหลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น
- 6.18 ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยของบริษัท โดยห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับของบริษัท ยกเว้นเป็นไปตามหลักเกณฑ์การเปิดเผยอย่างเป็นทางการของบริษัท รวมถึงการตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำไปใช้งาน
- 6.19 ผู้ใช้งานจะต้องใช้ระบบอินเทอร์เน็ต ในลักษณะที่ไม่เป็นการละเมิดของบุคคลอื่น ๆ และจะต้องไม่ก่อให้เกิดความเสียหายขึ้นต่อบริษัท รวมทั้งจะต้องไม่กระทำการใดอันเข้าข่ายความผิดตามพระราชบัญญัติว่าด้วยการกระทำ



ผลิตภัณฑ์คอมพิวเตอร์ หรือกฎหมายที่เกี่ยวข้องโดยเด็ดขาด ทั้งนี้ การใช้ระบบอินเทอร์เน็ตเพื่อการปฏิบัติงานของบริษัทในทุกกรณี ผู้ใช้งานจะต้องปฏิบัติตามขั้นตอนการปฏิบัติที่บริษัทกำหนดไว้อย่างเคร่งครัด

- 6.20 บริษัทจัดลำดับชั้นความลับ ต้องมีการแบ่งประเภทของข้อมูลตามภารกิจและการจัดลำดับความสำคัญของข้อมูล กำหนดวิธีบริหารจัดการกับข้อมูลแต่ละประเภท รวมถึงกำหนดวิธีปฏิบัติกับข้อมูลลับหรือข้อมูลสำคัญ ก่อนการยกเลิกหรือการนำกลับมาใช้ใหม่ โดยการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส ที่เป็นมาตรฐานสากล เช่น การใช้ Secure Socket Layer การใช้ Virtual Private Network เป็นต้น
- 6.21 บริษัทมีมาตรการควบคุมความถูกต้องของข้อมูลที่จัดเก็บ นำเข้า ประมวลผล และแสดงผล ในกรณีที่มีการจัดเก็บข้อมูลเดียวกันไว้หลายที่ หรือมีการจัดเก็บชุดข้อมูลที่มีความสัมพันธ์กัน ต้องมีการควบคุมให้ข้อมูลมีความถูกต้องครบถ้วนตรงกัน รวมถึงมาตรการรักษาความปลอดภัยข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของบริษัท เช่น ส่งซ่อม เป็นต้น หรือทำลายข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน
- 6.22 บริษัทมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยกำหนดสิทธิ์การใช้ข้อมูลและระบบสารสนเทศ เช่น สิทธิการใช้โปรแกรมระบบสารสนเทศ สิทธิการใช้งานอินเทอร์เน็ต เป็นต้น ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ โดยต้องให้สิทธิ์เฉพาะเท่าที่จำเป็นแก่การปฏิบัติหน้าที่ และได้รับความเห็นชอบจากผู้มีอำนาจหน้าที่เป็นลายลักษณ์อักษร รวมทั้งทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ
- 6.23 กรณีที่มีความจำเป็นที่ผู้ใช้งานซึ่งเป็นเจ้าของข้อมูลสำคัญมีการให้สิทธิ์ผู้ใช้งานรายอื่นให้สามารถเข้าถึงหรือแก้ไขเปลี่ยนแปลงข้อมูลของตนเองได้ เช่น การ Share Files เป็นต้น จะต้องเป็นการให้สิทธิ์เฉพาะรายหรือเฉพาะกลุ่มเท่านั้น และต้องยกเลิกการให้สิทธิ์ดังกล่าวในกรณีที่ไม่มีความจำเป็นแล้ว และเจ้าของข้อมูลต้องมีหลักฐานการให้สิทธิ์ดังกล่าว และต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- 6.24 กรณีที่มีความจำเป็นต้องให้สิทธิ์บุคคลอื่น ให้มีสิทธิ์ใช้งานระบบสารสนเทศและระบบเครือข่ายในลักษณะฉุกเฉินหรือชั่วคราว ต้องมีขั้นตอนหรือวิธีปฏิบัติ และต้องมีการขออนุมัติจากผู้มีอำนาจหน้าที่ทุกครั้ง บันทึกเหตุผลและความจำเป็น รวมถึงต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- 6.25 บริษัทมีระบบตรวจสอบตัวตนจริงและสิทธิ์การเข้าใช้งานของผู้ใช้งาน ก่อนเข้าสู่ระบบสารสนเทศที่รัดกุมเพียงพอ เช่น กำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น และต้องกำหนดให้ผู้ใช้งานแต่ละรายมีบัญชีผู้ใช้งานเป็นของตนเอง ทั้งนี้ การพิจารณาว่าการกำหนดรหัสผ่านมีความยากแก่การคาดเดาและการควบคุมการใช้รหัสผ่านมีความรัดกุมหรือไม่นั้น บริษัทจะใช้ปัจจัยดังต่อไปนี้ประกอบการพิจารณาในภาพรวม
- 6.26 พนักงาน
 - ควรกำหนดให้รหัสผ่านมีความยาวพอสมควร ซึ่งมาตรฐานสากลโดยส่วนใหญ่แนะนำให้มีความยาวขั้นต่ำ 8 ตัวอักษร (Alphabet + Numeric)
 - ควรใช้อักขระพิเศษประกอบ เช่น ; < > \$ @ # เป็นต้น

- สำหรับผู้ใช้งานทั่วไป ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 2 เดือน ส่วนผู้ใช้งานที่มีสิทธิ์พิเศษ เช่น ผู้จัดการระบบ (System Administrator) และผู้ใช้งานที่ติดมากับระบบ (Default User) เป็นต้น ควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 2 เดือน
- ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิม 3 ครั้งหลังสุด
- ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน หรือคาดเดาได้ง่าย เช่น "abcdef" "aaaaaa" "123456" "password" "P@ssw0rd" เป็นต้น
- ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อ นามสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น
- ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม
- ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ซึ่งในทางปฏิบัติโดยทั่วไปให้อยู่ที่ 5 ครั้ง หากการใส่รหัสผ่านผิดเกินจำนวนครั้งที่กำหนดไว้ระบบงานหรือโปรแกรมจะไม่อนุญาตหรือระงับการใช้งาน
- ควรมีวิธีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย เช่น การใส่ซองปิดผนึก เป็นต้น
- ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก หรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านนั้นโดยทันที
- ผู้ใช้งานควรเก็บรหัสผ่านไว้เป็นความลับ ไม่ควรจดใส่กระดาษแล้วติดไว้หน้าเครื่อง ทั้งนี้ ในกรณีที่มีการลวงรู้รหัสผ่านโดยบุคคลอื่น ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันที
- สำหรับกรณีผู้ใช้งานมีการใช้งานร่วมกันลักษณะ Shared Users Licenses เช่นระบบ SAP เป็นต้น ทางผู้ดูแลจะมีการส่งอีเมลแจ้งเตือนผู้รับผิดชอบการใช้งานให้ทำการเปลี่ยนรหัสผ่านในการเข้าระบบงานนั้น เมื่อมีการเปลี่ยนแปลงของผู้ใช้งานในสังกัด

6.27 บริษัทจัดให้มีระบบการตรวจสอบรายชื่อผู้ใช้งานของระบบงานสำคัญอย่างสม่ำเสมอ และดำเนินการตรวจสอบบัญชีรายชื่อผู้ใช้งานที่มีได้สิทธิ์ใช้งานระบบแล้ว เช่น บัญชีรายชื่อของผู้ใช้งานที่ลาออกแล้ว บัญชีรายชื่อที่ติดมากับระบบ เป็นต้น พร้อมทั้งระงับการใช้งานโดยทันทีเมื่อตรวจพบ เช่น Disable ลบออกจากระบบ หรือเปลี่ยนรหัสผ่าน เป็นต้น

6.28 บริษัทจัดให้มี Data Center Room ให้เป็นสัดส่วน เช่น แบ่งเป็นส่วนระบบเครือข่าย ส่วนเครื่องคอมพิวเตอร์แม่ข่าย ส่วนเครื่องสำรองไฟฟ้า ส่วนแบตเตอรี่เครื่องสำรองไฟฟ้า เป็นต้น เพื่อความสะดวกในการปฏิบัติงานและทำให้การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

6.29 บริษัทจัดทำข้อตกลงสำหรับการถ่ายโอนข้อมูล โดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ การรักษาความถูกต้องของข้อมูล และการรักษาความพร้อมที่จะให้บริการ โดยกำหนดให้มีการลงนามในสัญญาฯ ระหว่างบริษัทและหน่วยงานภายนอกว่าจะไม่เปิดเผยความลับของบริษัท ตลอดจนมีมาตรการในการติดตามและตรวจสอบการปฏิบัติงานและคุณภาพการให้บริการของผู้ให้บริการภายนอก ว่าเป็นไปตามสัญญาและข้อตกลง เช่น ผู้ให้บริการ Cloud บริษัทอาจตรวจสอบใบรับรองมาตรฐานคุณภาพ ISO 27000 จากเว็บไซต์ผู้ให้บริการเป็นระยะ เป็นต้น

7. หลักการเปิดเผย (Openness Principle)

บริษัทอาจเปิดเผยข้อมูลส่วนบุคคลของผู้มีส่วนได้เสียไม่ว่าจะเป็นในฐานะผู้ถือหุ้น พนักงาน คู่ค้าทางธุรกิจ ลูกค้า ให้แก่บุคคลหรือนิติบุคคลต่าง ๆ ตามที่ระดับด้านล่างนี้



- 7.1 บุคคลหรือนิติบุคคลที่เป็นเจ้าของผลิตภัณฑ์ (Brand) เพื่อประโยชน์ในการรวบรวมประวัติการสั่งซื้อสินค้า ซึ่งบริษัทจะเปิดเผยเฉพาะเจ้าของผลิตภัณฑ์ หรือเฉพาะแต่ข้อมูลส่วนบุคคลอันจำเป็นต่อการดำเนินการเท่านั้น
- 7.2 หน่วยงานราชการตามที่บริษัทต้องปฏิบัติตามประกาศ หลักเกณฑ์ บทบัญญัติของกฎหมาย ได้แก่ กรมสรรพากร สำนักงานประกันสังคม กรมพัฒนาธุรกิจการค้า สำนักงานคณะกรรมการคุ้มครองผู้บริโภค สำนักงานสวัสดิการและคุ้มครองแรงงาน กรมพัฒนาฝีมือแรงงาน
- 7.3 พันธมิตรของบริษัท บริษัทอาจเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลให้แก่บุคคลอื่นที่มีข้อตกลงเป็นพันธมิตรกับบริษัท เช่น สถาบันการเงิน บริษัทประกันภัย บริษัทหลักทรัพย์ บริษัทจัดการกองทุน เพื่อประโยชน์และสวัสดิการให้แก่ผู้มีส่วนได้เสีย
- 7.4 ผู้ให้บริการด้านที่วิชาชีพ ได้แก่ ที่ปรึกษาทางการเงิน ที่ปรึกษากฎหมาย ผู้สอบบัญชี ผู้ตรวจสอบภายใน
- 7.5 ผู้ให้บริการด้านโครงสร้างพื้นฐานและเทคโนโลยีสารสนเทศ การจัดเก็บข้อมูล ผู้ให้บริการคลาวด์
- 7.6 ผู้ให้บริการด้านการตลาด การจัดทำข้อมูลในเชิงสถิติ การโฆษณา การประชาสัมพันธ์ และการติดต่อสื่อสาร
- 7.7 บุคคลอื่นใดที่กฎหมายกำหนด ในกรณีที่มีกฎหมาย กฎเกณฑ์ ระเบียบต่าง ๆ ที่เกี่ยวข้อง คำสั่งของหน่วยงานราชการ หน่วยงานที่มีหน้าที่ในการกำกับดูแล หรือคำสั่งของหน่วยงานตุลาการให้บริษัทเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูล บริษัทจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลดังกล่าว
- 7.8 ผู้รับโอนสิทธิ และ/หรือหน้าที่จากบริษัท ในกรณีที่บริษัทประสงค์จะโอนสิทธิ และหน้าที่ของบริษัท รวมถึงการโอนกิจการบางส่วนหรือทั้งหมด การควบรวมกิจการ และการปรับเปลี่ยนโครงสร้างการถือหุ้นบริษัท บริษัทจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลให้แก่ผู้รับโอน (รวมถึงผู้ที่มีความเป็นไปได้ที่จะเป็นผู้รับโอน) โดยสิทธิและหน้าที่ของผู้รับโอนในส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลของเจ้าของข้อมูลจะเป็นไปตามนโยบาย ฯ ฉบับนี้ด้วย

8. หลักการมีส่วนร่วมของเจ้าของข้อมูล (Individual Participation Principle)

นอกเหนือจากสิทธิพื้นฐานของผู้มีส่วนได้เสียในการดำเนินธุรกิจของบริษัทในฐานะเจ้าของข้อมูลส่วนบุคคลที่บริษัทได้ทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล อันได้แก่ สิทธิในการได้รับแจ้งข้อมูล สิทธิในการเข้าถึงข้อมูล สิทธิในการแก้ไขข้อมูล สิทธิในการขอลบข้อมูล สิทธิในการจำกัดการให้ข้อมูล สิทธิในการได้รับแจ้งเตือนที่เกี่ยวข้องกับสิทธิต่าง ๆ สิทธิในการโอนย้ายข้อมูล สิทธิที่จะปฏิเสธการให้ใช้ข้อมูล สิทธิที่ไม่อนุญาตให้ใช้ระบบการตัดสินใจดำเนินการอัตโนมัติ แล้ว เจ้าของข้อมูลส่วนบุคคลยังมีสิทธิตามที่กฎหมายบัญญัติไว้เป็นการเฉพาะ ได้แก่

- 8.1 การให้ความยินยอม เจ้าของข้อมูลมีสิทธิเลือกที่จะให้ข้อมูลส่วนบุคคลใด ๆ ที่บริษัทร้องขอ และยินยอมให้บริษัทเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าวหรือไม่ก็ได้ เพียงแต่เจ้าของข้อมูลต้องรับทราบว่า การให้ข้อมูลส่วนบุคคลที่ไม่ครบถ้วนตามที่บริษัทร้องขอ หรือการไม่ให้ความยินยอมในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลดังกล่าว อาจทำให้เจ้าของข้อมูลถูกจำกัดสิทธิการใช้บริการบางอย่างของบริษัท หรือส่งผลให้

บริษัทไม่สามารถให้บริการแก่เจ้าของข้อมูลได้เลยหากข้อมูลดังกล่าวจำเป็นต่อบริษัทในการให้บริการแก่เจ้าของข้อมูล

- 8.2 การเข้าถึง และขอรับสำเนาข้อมูลส่วนบุคคลเหล่านั้น หรือขอให้บริษัทส่งข้อมูลส่วนบุคคลให้แก่เจ้าของข้อมูลเอง หรือผู้ควบคุมข้อมูลส่วนบุคคลอื่น (หากข้อมูลดังกล่าวอยู่ในรูปแบบที่สามารถดำเนินการดังกล่าวได้) รวมทั้งเจ้าของข้อมูลยังสามารถขอให้บริษัทเปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลของเจ้าของข้อมูลหากข้อมูลดังกล่าวเป็นข้อมูลที่เจ้าของข้อมูลไม่ได้ให้ความยินยอมในการจัดเก็บ
- 8.3 การคัดค้าน เจ้าของข้อมูลมีสิทธิคัดค้านการเก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเจ้าของข้อมูล หากข้อมูลนั้นบริษัทจัดเก็บได้โดยไม่ต้องได้รับความยินยอมจากเจ้าของข้อมูล หรือข้อมูลนั้นเก็บ ใช้ หรือเปิดเผยเพื่อการตลาดแบบตรง หรือการเพื่อการศึกษาวิจัย
- 8.4 การลบ ทำลาย หรือระงับการใช้ เจ้าของข้อมูลมีสิทธิร้องขอให้บริษัทลบ ทำลาย หรือระงับการใช้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่บริษัทเก็บรักษาไว้ หรือให้บริษัทดำเนินการให้ข้อมูลดังกล่าวกลายเป็นข้อมูลที่ไม่สามารถใช้ระบุตัวเจ้าของข้อมูลได้ หากเจ้าของข้อมูลเพิกถอน หรือคัดค้านการเก็บ ใช้ เปิดเผย ข้อมูลส่วนบุคคลที่เกี่ยวข้องกับเจ้าของข้อมูล หรือเมื่อไม่มีความจำเป็นที่จะต้องเก็บ ใช้ หรือ เปิดเผยตามวัตถุประสงค์ที่เจ้าของข้อมูลได้ให้ความยินยอมไว้ หรือเมื่อบริษัทไม่ปฏิบัติตามกฎหมายที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล
- 8.5 การแก้ไข เจ้าของข้อมูลมีสิทธิร้องขอให้บริษัทดำเนินการแก้ไขให้ข้อมูลส่วนบุคคลของเจ้าของข้อมูลที่บริษัทจัดเก็บไว้เป็นข้อมูลที่ถูกต้อง เป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด
- 8.6 การถอนความยินยอม เจ้าของข้อมูลมีสิทธิถอนความยินยอมในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลได้ แต่การถอนความยินยอมของเจ้าของข้อมูลจะไม่กระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่เจ้าของข้อมูลให้ความยินยอมไปแล้วก่อนหน้านี้ ทั้งนี้ การถอนความยินยอมดังกล่าวอาจทำให้บริษัทไม่สามารถให้บริการแก่เจ้าของข้อมูลต่อไปได้

ในการใช้สิทธิของเจ้าของข้อมูล เจ้าของข้อมูลรับทราบว่าสิทธิของเจ้าของข้อมูลในฐานะเจ้าของข้อมูลส่วนบุคคลที่ระบุไว้ในข้อ 8.1 ถึง 8.6 ข้างต้น เป็นสิทธิที่มีข้อจำกัดตามกฎหมายที่เกี่ยวข้อง และบริษัทอาจปฏิเสธการใช้สิทธิของเจ้าของข้อมูลหากบริษัทมีเหตุโดยชอบด้วยกฎหมายในการปฏิเสธการใช้สิทธิดังกล่าว

อย่างไรก็ตาม การใช้สิทธิในฐานะเจ้าของข้อมูลส่วนบุคคลตามที่ระบุไว้ในเอกสารฉบับนี้ ย่อมจำกัดไว้แต่เพียงแต่การให้บริการพื้นฐานที่ไม่ทำให้ผู้ควบคุมข้อมูลส่วนบุคคลเกิดค่าใช้จ่ายที่เกินความจำเป็น หากการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลของผู้เกี่ยวข้องได้ก่อให้เกิดความเสียหาย ค่าธรรมเนียม ค่าใช้จ่ายเพื่อการดำเนินการตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคล เจ้าของข้อมูลส่วนบุคคลจะต้องรับผิดชอบใช้คืนเงินค่าดำเนินการต่าง ๆ ที่มีการขอใช้สิทธิเช่นนั้น

9. หลักการความรับผิดชอบ (Accountability Principle)

9.1 ระยะเวลาที่บริษัทจัดเก็บข้อมูลส่วนบุคคลของเจ้าของข้อมูล



SINO

LOGISTICS CORPORATION

นอกจากจะมีการระบุไว้เป็นการเฉพาะตามที่กฎหมายกำหนดไว้ บริษัทจะจัดเก็บข้อมูลส่วนบุคคลของผู้มีส่วนได้เสียกับการดำเนินธุรกิจเป็นระยะเวลา 10 ปีนับจากที่ผู้มีส่วนได้เสียดังกล่าวสิ้นสุดนิติสัมพันธ์กับบริษัท เว้นแต่กรณีเป็นความจำเป็นที่เกี่ยวข้องกับการใช้หรือการได้สิทธิเรียกร้องตามกฎหมาย การบังคับคดี การวางทรัพย์ หรือตามที่กฎหมายกำหนดไว้เป็นการเฉพาะ

9.2 ระบบการตรวจสอบถึงการลบ ทำลายข้อมูลส่วนบุคคลที่พ้นระยะเวลาจัดเก็บ

บริษัทได้จัดให้มีระบบตรวจสอบเพื่อลบหรือทำลายข้อมูลส่วนบุคคลของผู้มีส่วนได้เสีย เมื่อพ้นกำหนดระยะเวลาจัดเก็บ หรือไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือขอลงความยินยอม เว้นแต่เป็นกรณีที่บริษัทต้องทำการเก็บรักษาเพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็น หรือเป็นไปตามข้อยกเว้นของกฎหมายที่บัญญัติไว้เป็นการเฉพาะ รวมถึงการใช้เพื่อการก่อสร้างสิทธิเรียกร้องตามกฎหมาย หรือเพื่อเป็นการปฏิบัติตามการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย หรือเพื่อการปฏิบัติตามกฎหมาย

9.3 ข้อมูลเกี่ยวกับบริษัทในฐานะผู้ควบคุมข้อมูลส่วนบุคคล

หากเจ้าของข้อมูลประสงค์จะติดต่อบริษัท เพื่อใช้สิทธิเกี่ยวกับข้อมูลส่วนบุคคลของเจ้าของข้อมูล หรือหากเจ้าของข้อมูลมีข้อสงสัยอื่นใดเกี่ยวกับข้อมูลส่วนบุคคลของเจ้าของข้อมูล เจ้าของข้อมูลสามารถติดต่อบริษัทได้ตามรายละเอียดดังต่อไปนี้

ผู้ควบคุมข้อมูลส่วนบุคคล

บริษัท ไชน่ โลจิสติกส์ คอร์ปอเรชั่น จำกัด (มหาชน)

สำนักงานใหญ่ตั้งอยู่เลขที่ 1011 อาคารศุภาสัย แกรนด์ ทาวเวอร์ ชั้น 7 ยูนิต 05 ถนนพระราม 3 แขวงช่องนนทรี เขตยานนาวา กรุงเทพมหานคร

โทรศัพท์ : 02-6870477

E-mail address: nanmanus.w@sinologistics.co.th

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

นางสาวสุภาวดี จันทร์กิตติพร

วันทำการปกติ โทรศัพท์ 02-6870477 เวลาติดต่อ 08.30-17.30 น.

วันหยุดทำการ โทรศัพท์ 084-7628023 ตลอด 24 ชั่วโมง