นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy)
บริษัท เอ็นบีดี เฮลท์แคร์ จำกัด และบริษัทย่อย

---

1. บทนำ

บริษัท เอ็นบีดี เฮลท์แคร์ จำกัด และบริษัทย่อย ได้แก่ **บริษัท โปรโนวา แลบบอราทอรีส์ จำกัด บริษัท นูทริน่า อินเตอร์ฟู้ดส์ จำกัด** และ **บริษัท ดีเอสซี ซินดิเคท จำกัด** รวมถึงบุคคลที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของบริษัท เอ็นบีดี เฮลท์แคร์ จำกัด และบริษัทย่อย ซึ่งต่อไปนี้ จะเรียกรวมว่า **"บริษัทฯ"** ได้ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลและข้อมูลอื่นอันเกี่ยวกับท่าน (รวมเรียกว่า **"ข้อมูล"**) เพื่อให้ท่านสามารถเชื่อมั่นได้ว่า บริษัทฯ มีความโปร่งใสและความรับผิดชอบในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 (**"กฎหมายคุ้มครองข้อมูลส่วนบุคคล"**) รวมถึงกฎหมายอื่นที่เกี่ยวข้อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล (**"นโยบาย"**) นี้ จึงได้ถูกจัดทำขึ้นเพื่อชี้แจงแก่ท่านถึงรายละเอียดเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผย (รวมเรียกว่า **"ประมวลผล"**) ข้อมูลส่วนบุคคลซึ่งดำเนินการโดยบริษัทฯ รวมถึงเจ้าหน้าที่และบุคคลที่เกี่ยวข้องผู้ดำเนินการแทน หรือในนามของบริษัทฯ โดยมีเนื้อหาสาระดังต่อไปนี้

2. ขอบเขตการบังคับใช้นโยบาย

นโยบายนี้ ใช้บังคับกับข้อมูลส่วนบุคคลของบุคคลซึ่งมีความสัมพันธ์กับบริษัทฯ ในปัจจุบันและที่อาจมีในอนาคต ซึ่งถูกประมวลผลข้อมูลส่วนบุคคลโดยบริษัทฯ เจ้าหน้าที่ พนักงานตามสัญญา หน่วยธุรกิจ หรือหน่วยงานรูปแบบอื่นที่ดำเนินการโดยบริษัทฯ และรวมถึงคู่สัญญา หรือบุคคลภายนอกที่ประมวลผลข้อมูลส่วนบุคคลแทน หรือในนามของบริษัทฯ (**"ผู้ประมวลผลข้อมูลส่วนบุคคล"**) ภายใต้ผลิตภัณฑ์และบริการต่าง ๆ เช่น เว็บไซต์ ระบบ แอปพลิเคชัน เอกสาร หรือบริการในรูปแบบอื่นที่ควบคุมดูแลโดยบริษัทฯ (รวมเรียกว่า **"บริการ"**)

บุคคลมีความสัมพันธ์กับบริษัทฯ ตามความในวรรคแรก รวมถึง

1) ลูกค้าบุคคลธรรมดา
2) เจ้าหน้าที่ หรือผู้ปฏิบัติงาน ลูกจ้าง
3) คู่ค้าและผู้ให้บริการซึ่งเป็นบุคคลธรรมดา
4) กรรมการ ผู้รับมอบอำนาจ ผู้แทน ตัวแทน ผู้ถือหุ้น ลูกจ้าง หรือบุคคลอื่นที่มีความสัมพันธ์ในรูปแบบเดียวกันของนิติบุคคลที่มีความสัมพันธ์กับบริษัทฯ
5) ผู้ใช้งานผลิตภัณฑ์ หรือบริการของบริษัทฯ
6) ผู้เข้าชม หรือใช้งานเว็บไซต์ https://www.nbd.co.th/th รวมทั้งระบบ แอปพลิเคชัน อุปกรณ์ หรือช่องทางการสื่อสารอื่นซึ่งควบคุมดูแลโดยบริษัทฯ
7) บุคคลอื่นที่บริษัทฯ เก็บรวบรวมข้อมูลส่วนบุคคล เช่น ผู้สมัครงาน ครอบครัวของเจ้าหน้าที่ ผู้ค้ำประกัน ผู้รับประโยชน์ในกรมธรรม์ประกันภัย เป็นต้น

ข้อ 1) ถึง 7) เรียกรวมกันว่า **"ท่าน"**

นอกจากนโยบายฉบับนี้แล้ว บริษัทฯ อาจกำหนดให้มี**คำประกาศนโยบายความเป็นส่วนตัว** (**"ประกาศ"**) สำหรับผลิตภัณฑ์หรือบริการของบริษัทฯ เพื่อชี้แจงให้เจ้าของข้อมูลส่วนบุคคล ซึ่งเป็นผู้ใช้บริการได้ทราบถึงข้อมูลส่วนบุคคลที่ถูกประมวลผล วัตถุประสงค์และเหตุผลอันชอบด้วยกฎหมายในการประมวลผล ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล รวมถึงสิทธิในข้อมูลส่วนบุคคลที่เจ้าของข้อมูลส่วนบุคคลพึงมีในผลิตภัณฑ์ หรือบริการนั้นเป็นการเฉพาะเจาะจง

ทั้งนี้ ในกรณีที่มีความขัดแย้งกันในสาระสำคัญระหว่างความในประกาศเกี่ยวกับความเป็นส่วนตัวและนโยบายนี้ ให้ถือตามความในประกาศเกี่ยวกับความเป็นส่วนตัวของบริการนั้น

3. คำนิยาม

- **ข้อมูลส่วนบุคคล** หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
- **ข้อมูลส่วนบุคคลอ่อนไหว** หมายถึง ข้อมูลส่วนบุคคลตามที่ถูกบัญญัติไว้ในมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ซึ่งได้แก่ ข้อมูลเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด
- **การประมวลผลข้อมูลส่วนบุคคล** หมายถึง การดำเนินการใด ๆ กับข้อมูลส่วนบุคคล เช่น เก็บรวบรวม บันทึก สำเนา จัดระเบียบ เก็บรักษา ปรับปรุง เปลี่ยนแปลง ใช้ กู้คืน เปิดเผย ส่งต่อ เผยแพร่ โอน รวม ลบ ทำลาย เป็นต้น
- **เจ้าของข้อมูลส่วนบุคคล** หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่บริษัทฯ เก็บรวบรวม ใช้ หรือเปิดเผย
- **ผู้ควบคุมข้อมูลส่วนบุคคล** หมายถึง บุคคล หรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
- **ผู้ประมวลผลข้อมูลส่วนบุคคล** หมายถึง บุคคล หรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคล หรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

4. แหล่งที่มาของข้อมูลส่วนบุคคลที่บริษัทฯ เก็บรวบรวม

บริษัทฯ เก็บรวบรวม หรือได้มาซึ่งข้อมูลส่วนบุคคลประเภทต่าง ๆ จากแหล่งข้อมูล ดังต่อไปนี้

1) **ข้อมูลส่วนบุคคลที่บริษัทฯ เก็บรวบรวมจากเจ้าของข้อมูลส่วนบุคคลโดยตรงในช่องทางให้บริการต่าง ๆ** เช่น ขั้นตอนการสมัคร ลงทะเบียน สมัครงาน ลงนามในสัญญา เอกสาร ทำแบบสำรวจ หรือใช้งานผลิตภัณฑ์ บริการ หรือช่องทางให้บริการอื่นที่ควบคุมดูแลโดยบริษัทฯ หรือเมื่อเจ้าของข้อมูลส่วนบุคคลติดต่อสื่อสารกับบริษัทฯ ณ ที่ทำการ หรือผ่านช่องทางติดต่ออื่นที่ควบคุมดูแลโดยบริษัทฯ เป็นต้น

2) **ข้อมูลที่บริษัทฯ เก็บรวบรวมจากการที่เจ้าของข้อมูลส่วนบุคคลเข้าใช้งานเว็บไซต์ ผลิตภัณฑ์ หรือบริการ อื่น ๆ ตามสัญญา หรือตามพันธกิจ** เช่น การติดตามพฤติกรรมการใช้งานเว็บไซต์ ผลิตภัณฑ์ หรือบริการของบริษัทฯ ด้วยการใช้คุกกี้ (Cookie) หรือจากซอฟต์แวร์บนอุปกรณ์ของเจ้าของข้อมูลส่วนบุคคล เป็นต้น

3) **ข้อมูลส่วนบุคคลที่บริษัทฯ เก็บรวบรวมจากแหล่งอื่นนอกจากเจ้าของข้อมูลส่วนบุคคล โดยที่แหล่งข้อมูลดังกล่าวมีอำนาจหน้าที่ มีเหตุผลที่ชอบด้วยกฎหมาย หรือได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลแล้วในการเปิดเผยข้อมูลแก่บริษัทฯ** เช่น การเชื่อมโยงบริการดิจิทัลของหน่วยงานของรัฐในการให้บริการเพื่อประโยชน์สาธารณะแบบเบ็ดเสร็จแก่เจ้าของข้อมูลส่วนบุคคลเอง การรับข้อมูลส่วนบุคคลจากหน่วยงานของรัฐแห่งอื่นในฐานะที่บริษัทฯ มีหน้าที่ตามพันธกิจในการดำเนินการจัดให้มีศูนย์แลกเปลี่ยนข้อมูลกลางเพื่อสนับสนุนการดำเนินการของหน่วยงานของรัฐในการให้บริการประชาชนผ่านระบบดิจิทัล รวมถึงจากความจำเป็นเพื่อให้บริการตามสัญญาที่อาจมีการแลกเปลี่ยนข้อมูลส่วนบุคคลกับหน่วยงานคู่สัญญาได้

นอกจากนี้ ยังหมายความรวมถึง กรณีที่ท่านเป็นผู้ให้ข้อมูลส่วนบุคคลของบุคคลภายนอกแก่บริษัทฯ ดังนั้น ท่านมีหน้าที่รับผิดชอบในการแจ้งรายละเอียดตามนโยบายนี้ หรือประกาศของผลิตภัณฑ์ หรือบริการ ตามแต่กรณี ให้บุคคลดังกล่าวทราบตลอดจนขอความยินยอมจากบุคคลนั้น หากเป็นกรณีที่ต้องได้รับความยินยอมในการเปิดเผยข้อมูลแก่บริษัทฯ

ทั้งนี้ ในกรณีที่เจ้าของข้อมูลส่วนบุคคลปฏิเสธไม่ให้ข้อมูลที่มีความจำเป็นในการให้บริการของบริษัทฯ อาจเป็นผลให้บริษัทฯ ไม่สามารถให้บริการนั้นแก่เจ้าของข้อมูลส่วนบุคคลดังกล่าวได้ทั้งหมด หรือบางส่วน

5. การเก็บรวบรวมข้อมูลส่วนบุคคล

โดยบริษัทฯ จะดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลเมื่อได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลก่อน ยกเว้นในกรณีดังต่อไปนี้

1. เพื่อปฏิบัติตามสัญญา กรณีการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อความจำเป็นต่อการให้บริการ หรือปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลและบริษัทฯ
2. เพื่อป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพ
3. เพื่อปฏิบัติตามกฎหมาย
4. เพื่อผลประโยชน์อันชอบโดยกฎหมายของบริษัทฯ กรณีมีความจำเป็นเพื่อประโยชน์อันชอบธรรมในการดำเนินงานของบริษัทฯ โดยบริษัทฯ จะพิจารณาถึงสิทธิของเจ้าของข้อมูลเป็นสำคัญ เช่น เพื่อป้องกันการฉ้อโกง การรักษาความปลอดภัยในระบบเครือข่าย การปกป้องสิทธิเสรีภาพและประโยชน์ของเจ้าของข้อมูลเป็นต้น
5. เพื่อการศึกษาวิจัย หรือสถิติ กรณีที่มีการจัดทำเอกสารประวัติศาสตร์ หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษาวิจัย หรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิ และเสรีภาพของเจ้าของข้อมูล
6. เพื่อปฏิบัติภารกิจของรัฐ กรณีมีความจำเป็นต่อการปฏิบัติตามภารกิจเพื่อประโยชน์สาธารณะ หรือการปฏิบัติหน้าที่ตามอำนาจรัฐที่บริษัทฯ ได้รับมอบหมาย

ในกรณีที่บริษัทฯ มีความจำเป็นต้องเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเพื่อการปฏิบัติตามสัญญา การปฏิบัติหน้าที่ตามกฎหมาย หรือเพื่อความจำเป็นในการเข้าทำสัญญา หากท่านปฏิเสธไม่ให้ข้อมูลส่วนบุคคล หรือคัดค้านการดำเนินการประมวลผลตามวัตถุประสงค์ของกิจกรรม อาจมีผลทำให้บริษัทฯ ไม่สามารถดำเนินการ หรือให้บริการตามที่ท่านร้องขอได้ทั้งหมด หรือบางส่วน

6. ประเภทของข้อมูลส่วนบุคคลที่บริษัทฯ เก็บรวบรวม

ในการเก็บรวบรวม และเก็บรักษาข้อมูลส่วนบุคคล บริษัทฯ จะใช้วิธีการที่ชอบด้วยกฎหมายและจำกัดเพียงเท่าที่จำเป็นตามวัตถุประสงค์การดำเนินงานของบริษัทฯ อันประกอบด้วย

ประเภทข้อมูลส่วนบุคคล	รายละเอียดและตัวอย่าง
ข้อมูลเฉพาะตัวบุคคล	ข้อมูลระบุชื่อเรียกของท่าน หรือข้อมูลจากที่ระบุข้อมูลเฉพาะตัวของท่าน เช่น ชื่อ-นามสกุล อายุ วันเดือนปีเกิด สัญชาติ หมายเลขบัตรประจำตัวประชาชน หรือหมายเลขหนังสือเดินทาง หรือเอกสารราชการอื่น ๆ ที่สามารถระบุตัวตนได้ เป็นต้น
ข้อมูลสำหรับการติดต่อ	ข้อมูลสำหรับการติดต่อท่าน เช่น ที่อยู่ หมายเลขโทรศัพท์ อีเมล ชื่อบัญชี Social media เป็นต้น
ข้อมูลเอกสารทางราชการ	ข้อมูลเอกสารราชการของท่าน เช่น สำเนาบัตรประจำตัวประชาชน สำเนาทะเบียนบ้าน สำเนาหนังสือเดินทาง สำเนาสูติบัตร เป็นต้น
ข้อมูลทางการเงิน	ข้อมูลทางการเงินของท่าน เช่น เลขบัญชีธนาคาร สำเนาหน้าสมุดบัญชีธนาคาร ข้อมูลเลขบัตรเครดิต รายได้ เป็นต้น
ข้อมูลที่ได้จากเก็บรวบรวมของบริษัทฯ หรือระบบอัตโนมัติจากอุปกรณ์ต่าง ๆ ของบริษัทฯ	ข้อมูลที่ได้จากเก็บรวบรวมของบริษัทฯ หรือระบบอัตโนมัติจากอุปกรณ์ ต่าง ๆ ของบริษัทฯ เช่น รหัสพนักงาน หมายเลขใบอนุญาตเข้าทำงาน ภาพจากกล้องวงจรปิด เป็นต้น
ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน	ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนของท่าน เช่น เชื้อชาติ ข้อมูลศาสนา ข้อมูลความพิการ ประวัติอาชญากรรม ข้อมูลชีวภาพ (ข้อมูลจำลองลายนิ้วมือ ข้อมูลภาพจำลองใบหน้า) ข้อมูลเกี่ยวกับสุขภาพ เป็นต้น

7. คุกกี้

บริษัทฯ เก็บรวบรวมและใช้คุกกี้ (Cookie) รวมถึงเทคโนโลยีอื่นในลักษณะเดียวกันในเว็บไซต์ที่อยู่ภายใต้ความดูแลของบริษัทฯ เช่น https://www.nbd.co.th/th หรือบนอุปกรณ์ของท่านตามแต่บริการที่ท่านใช้งาน ทั้งนี้ เพื่อการดำเนินการด้านความปลอดภัยในการให้บริการของบริษัทฯ และเพื่อให้ท่านซึ่งเป็นผู้ใช้งานได้รับความสะดวกและประสบการณ์ที่ดีในการใช้งานบริการของบริษัทฯ และข้อมูลเหล่านี้ จะถูกนำไปเพื่อปรับปรุงเว็บไซต์ของบริษัทฯ ให้ตรงกับความต้องการของท่านมากยิ่งขึ้น โดยท่านสามารถตั้งค่า หรือลบการใช้งานคุกกี้ได้ด้วยตนเองจากการตั้งค่าในเว็บเบราว์เซอร์ (Web Browser) ของท่าน

8. วัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล

บริษัทฯ ดำเนินการเก็บรวบรวมข้อมูลส่วนบุคคลของท่านเพื่อวัตถุประสงค์หลายประการ ซึ่งขึ้นอยู่กับประเภทของผลิตภัณฑ์หรือบริการ หรือกิจกรรมที่ท่านใช้บริการ ตลอดจนลักษณะความสัมพันธ์ของท่านกับบริษัทฯ หรือข้อพิจารณาในแต่ละบริบทเป็นสำคัญ โดยวัตถุประสงค์ที่ระบุไว้ดังต่อไปนี้เป็นเพียงกรอบการใช้ข้อมูลส่วนบุคคลของบริษัทฯ เป็นการทั่วไป ทั้งนี้ เฉพาะวัตถุประสงค์ที่เกี่ยวข้องกับผลิตภัณฑ์ หรือบริการที่ท่านใช้งาน หรือมีความสัมพันธ์ด้วยเท่านั้นที่จะมีผลบังคับใช้กับข้อมูลของท่าน

1. เพื่อเข้าทำสัญญา หรือปฏิบัติหน้าที่ตามสัญญาระหว่างบริษัทฯ กับเจ้าของข้อมูล หรือปฏิบัติหน้าที่ตามสัญญาระหว่างบริษัทฯ กับบุคคลภายนอกเพื่อประโยชน์ของเจ้าของข้อมูล
2. เพื่อตอบคำถามและให้ความช่วยเหลือแก่เจ้าของข้อมูล
3. เพื่อพัฒนาและปรับปรุงสินค้า ผลิตภัณฑ์ และบริการของบริษัทฯ ให้ตอบสนองต่อความต้องการของเจ้าของข้อมูลมากยิ่งขึ้น
4. เพื่อให้ข้อมูลและแนะนำสินค้า ผลิตภัณฑ์ การบริการ หรือประชาสัมพันธ์ทางการตลาด รายการส่งเสริมการขาย หรือสิทธิประโยชน์ผ่านช่องทางการติดต่อที่ได้รับจากเจ้าของข้อมูล ตามที่เจ้าของข้อมูลได้ให้คำยินยอม ตามที่ท่านได้ยินยอมกับทางบริษัทฯ
5. เพื่อสำรวจความคิดเห็น วิเคราะห์ การทำวิจัย และจัดทำข้อมูลทางสถิติ เพื่อใช้ทางการตลาด หรือการพัฒนาและปรับปรุงการดำเนินกิจการของบริษัทฯ ตามที่ท่านได้ยินยอมกับทางบริษัทฯ
6. เพื่อประโยชน์ในการบริหารจัดการงาน หรือดำเนินงานภายในของบริษัทฯ ที่จำเป็นภายใต้ประโยชน์โดยชอบด้วยกฎหมาย
7. เพื่อตรวจสอบ กำกับดูแล และรักษาความปลอดภัยบริเวณอาคาร หรือสถานที่ของบริษัทฯ
8. เพื่อการปฏิบัติตามกฎหมายที่เกี่ยวข้องกับการดำเนินงานของบริษัทฯ เช่น การหักภาษี ณ ที่จ่าย เป็นต้น
9. เพื่อให้ข้อมูลแก่หน่วยงานของรัฐที่มีอำนาจหน้าที่ตามกฎหมายตามที่หน่วยงานภาครัฐร้องขอ เช่น สำนักงานตำรวจแห่งชาติ สำนักงานป้องกันและปราบปรามการฟอกเงิน กรมสรรพากร ศาล เป็นต้น
10. เพื่อดำเนินกิจกรรมใด ๆ ทางบัญชีและการเงิน เช่น การตรวจสอบบัญชี การแจ้งและเรียกเก็บหนี้ การใช้สิทธิสวัสดิการต่าง ๆ ภาษี และหลักฐานการดำเนินธุรกรรมต่าง ๆ ที่กฎหมายกำหนด
11. เพื่อประโยชน์อันชอบด้วยกฎหมายของบริษัทฯ เช่น การบันทึกเสียงการร้องเรียนผ่านระบบ Call Center การบันทึกภาพผ่านกล้อง CCTV เป็นต้น
12. เพื่อใช้ในการสอบสวนและปฏิบัติตามกฎหมาย ข้อบังคับ ระเบียบ หรือหน้าที่ตามกฎหมายของบริษัทฯ
13. ใช้ข้อมูลในการยืนยันตัวตนลูกค้า
14. วัตถุประสงค์อื่น ๆ ที่ได้รับคำยินยอมชัดแจ้งจากท่าน

9. การส่งต่อและเปิดเผยข้อมูลส่วนบุคคล

บริษัทฯ จะไม่เปิดเผยและส่งต่อข้อมูลส่วนบุคคลของท่านไปยังหน่วยงานภายนอก เว้นแต่ได้รับคำยินยอมชัดแจ้งจากท่าน หรือเป็นไปตามกรณีดังต่อไปนี้

1. เพื่อบรรลุวัตถุประสงค์ตามที่ระบุในนโยบายความเป็นส่วนตัวฉบับนี้ บริษัทฯ อาจจำเป็นต้องเปิดเผยหรือแบ่งปันข้อมูลเฉพาะเท่าที่จำเป็นแก่คู่ค้า ผู้ให้บริการ หรือหน่วยงานภายนอก โดยบริษัทฯ จะจัดทำข้อตกลงการประมวลผลข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

2. บริษัทฯ อาจเปิดเผย หรือแบ่งปันข้อมูลส่วนบุคคลให้แก่ หน่วยงานภายใต้ หรือในเครือของบริษัทฯ โดยจะเป็นการประมวลผลข้อมูลภายใต้วัตถุประสงค์ที่ระบุในนโยบายความเป็นส่วนตัวฉบับนี้เท่านั้น
3. กฎหมาย หรือกระบวนการทางกฎหมายบังคับให้เปิดเผยข้อมูล หรือเปิดเผยต่อเจ้าพนักงาน เจ้าหน้าที่รัฐ หรือหน่วยงานที่มีอำนาจเพื่อปฏิบัติตามคำสั่งหรือคำขอที่ชอบด้วยกฎหมาย

10. การถ่ายโอนหรือส่งต่อข้อมูลไปยังต่างประเทศ

บริษัทฯ อาจจะส่งหรือโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ โดยจะทำให้แน่ใจว่าประเทศปลายทางหรือหน่วยงานปลายทางมีมาตรฐานและนโยบายในการคุ้มครองความเป็นส่วนตัวที่เพียงพอ

อย่างไรก็ดี ในกรณีที่ประเทศปลายทางไม่มีมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอการถ่ายโอน หรือส่งต่อข้อมูลดังกล่าว บริษัทฯ จะดำเนินการตามหลักเกณฑ์และวิธีการตามมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลที่เพียงพอจะต้องเป็นไปตามข้อยกเว้นตามหลักเกณฑ์ที่ บริษัทฯ กำหนดโดยไม่ขัดต่อกฎหมาย

11. ระยะเวลาในการเก็บรวบรวมข้อมูลส่วนบุคคลของท่าน

บริษัทฯ จะเก็บรักษาข้อมูลส่วนบุคคลของท่านไว้ในระยะเวลาเท่าที่ข้อมูลนั้นยังมีความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลเท่านั้น ตามรายละเอียดที่ได้กำหนดไว้ในนโยบาย ประกาศ หรือตามกฎหมายที่เกี่ยวข้อง ทั้งนี้ เมื่อพ้นระยะเวลาและข้อมูลส่วนบุคคลของท่านสิ้นความจำเป็นตามวัตถุประสงค์ดังกล่าวแล้ว บริษัทฯ จะทำการลบ ทำลายข้อมูลส่วนบุคคลของท่าน หรือทำให้ข้อมูลส่วนบุคคลของท่านไม่สามารถระบุตัวตนได้ต่อไป ตามรูปแบบและมาตรฐานการลบทำลายข้อมูลส่วนบุคคล อย่างไรก็ดี ในกรณีที่มีข้อพิพาท การใช้สิทธิหรือคดีความอันเกี่ยวข้องกับข้อมูลส่วนบุคคลของท่าน บริษัทฯ ขอสงวนสิทธิในการเก็บรักษาข้อมูลนั้นต่อไปจนกว่าข้อพิพาทนั้นจะได้มีคำสั่ง หรือคำพิพากษาถึงที่สุด

ชื่อกิจกรรม	ระยะเวลาการเก็บ		สถานที่จัดเก็บ
เก็บข้อมูลประวัติพนักงาน	ตามระยะดำเนินงานบริษัท	*	แฟ้มประวัติพนักงาน,ระบบ Biosoft
การรับสมัครพนักงาน	1	ปี	แฟ้มประวัติผู้สมัครงาน, files server
การจัดเก็บสัญญาการจ้างงาน	5	ปี	แฟ้มประวัติพนักงาน, files server
ประวัติพนักงานลาออก	5	ปี	แฟ้มประวัติพนักงานลาออก
การเก็บประวัติผู้ค้ำประกัน	5	ปี	แฟ้มประวัติพนักงาน, files server
การจัดกิจกรรมสันทนาการประจำปี	5	ปี	แฟ้มการจัดกิจกรรมสันทนาการประจำปี, files server
การจัดทำสัญญาจ้างงานคนพิการ	ตามระยะดำเนินงานบริษัท	*	แฟ้มเอกสารสัญญาจ้างคนพิการ, files server
การบันทึกการเข้างานของพนักงาน	ตามระยะดำเนินงานบริษัท	*	ระบบ HIP
การจัดทำประกันชีวิต/อุบัติเหตุของพนักงาน	5	ปี	แฟ้มประกันสุขภาพ, แฟ้มประกันอุบัติเหตุ
การตรวจร่างกายประจำปี	5	ปี	รายงานรวม, CD, ไฟล์ Excel ใน CD
การหักเงินนำส่งกรมบังคับคดี	ตามระยะดำเนินงานบริษัท	*	แฟ้มเอกสาร
การหักเงินเดือนให้แก่ กยศ.	ตามระยะดำเนินงานบริษัท	*	แฟ้มเอกสาร, files server
การฝึกอบรมพนักงาน	ตามระยะดำเนินงานบริษัท	*	แฟ้มการจัดอบรม, ระบบ AX
เก็บสำเนาสัญญาที่ปรึกษา	ตามระยะดำเนินงานบริษัท	*	เอกสารสัญญา,files server
สัญญาจ้างบริการ แม่บ้าน รปภ.	5	ปี	files server, แฟ้มสัญญา
การเช่าระบบโทรศัพท์ (สัญญา)	5	ปี	แฟ้มสัญญา, files server
การจัดทำหนังสือรับรองหัก ณ จ่าย	10	ปี	แฟ้ม ภงด 3, ระบบ ERP AX
การทำจ่ายผ่านทางเช็ค	10	ปี	แฟ้มรายการใบสำคัญจ่าย, ระบบ ERP AX

ชื่อกิจกรรม	ระยะเวลาการเก็บ		สถานที่จัดเก็บ
เก็บข้อมูลรหัสผู้จำหน่ายใหม่ (Vender)	10	ปี	แฟ้มรหัสผู้จำหน่ายใหม่ (Vender)
การจัดทำใบแจ้งหนี้/จัดทำใบเสร็จรับเงิน/ใบกำกับภาษี	10	ปี	แฟ้มรายงานภาษีขาย, ระบบ ERP AX
การจัดเก็บเอกสารใบเคลียร์เงินสดย่อย	10	ปี	แฟ้มรายการใบสำคัญจ่าย, ระบบ ERP AX
การออกใบเสร็จรับเงินให้พนักงาน	10	ปี	แฟ้มรายการใบสำคัญจ่าย, ระบบ ERP AX
การจัดทำสัญญา/หนังสือมอบอำนาจ	10	ปี	แฟ้มเอกสารสัญญา, files server
การทำจ่ายผ่านการโอนเงิน /คืนเงินให้ลูกค้า	10	ปี	แฟ้มรายการใบสำคัญจ่าย, ระบบ ERP AX
การเก็บประวัติเจ้าหน้าที่รัฐที่เข้ามาตรวจสอบ	10	ปี	แฟ้มข้อมูลการเข้าตรวจสอบของหน่วยงานรัฐ
เก็บข้อมูลรหัสลูกค้าใหม่ (Customer)	10	ปี	แฟ้มรหัสลูกค้าใหม่ (Customer)
การเปิดหน้าบัญชีลูกค้าใหม่	1	ปี	Drive U
ส่งรายละเอียดและประสานงานกับห้างฯ/ร้าน	ตามระยะดำเนินงานบริษัท	*	files server
เบิกเงินค่าอาหารและเครื่องดื่ม/ค่าชั้นวางสินค้า/ค่าเชียร์สินค้า/ค่าภาษีป้าย	10	ปี	Drive U, เก็บที่ฝ่ายบัญชี
จัดทำสัญญา TTA (ซื้อขาย)	3	ปี	Drive R, เอกสารสัญญา
ส่งข่าวสารและโปรโมชั่นให้ลูกค้า	ตามระยะดำเนินงานบริษัท	*	files server
การจัดส่งของรางวัลให้ลูกค้า	1	ปี	อีเมลบริษัท, เก็บที่ฝ่ายบัญชี เพื่อหัก ณ ที่จ่าย
เก็บข้อมูลลูกค้าจาก Platform E-commerce	10	ปี	Google Drive, ไฟล์ Excel ใน CD
การทำสัญญาจ้างพรีเซนเตอร์	10	ปี	แฟ้มเอกสารสัญญา, Personal Computer / E-mail
ระบบบริหารลูกค้าสัมพันธ์ CRM	10	ปี	ระบบ CRM, Google Drive
เกิจกรรมทางการตลาด Online/Offline	10	ปี	Google Drive
เก็บข้อมูลคนที่เข้ามาใช้ own media (Website, FB, Line)	10	ปี	ระบบ CRM, Google Drive
ส่งข่าวสารและโปรโมชั่นให้ลูกค้า	10	ปี	Google Drive, ระบบ CRM
การเบิก ยืม คืน อุปกรณ์ไอที	1	ปี	รายการยืมอุปกรณ์ IT
การ Backup ข้อมูล (File Sharing, database ERP)	ตามระยะดำเนินงานบริษัท	*	ห้อง Server, DR side
ข้อมูลลูกค้า	ตามระยะดำเนินงานบริษัท	*	Database Server
เก็บสำเนาสัญญา	1	ปี	เอกสารสัญญาบริการ,files server
การเก็บข้อมูลภาพกล้องวงจรปิด CCTV	30	วัน	NVR, DVR
แก้ไขข้อมูลในระบบ AX	5	ปี	File Sharing
แจ้งซ่อมอุปกรณ์ IT	ตามระยะดำเนินงานบริษัท	*	NBD website (Help desk database)

* ตามระยะดำเนินงานบริษัทฯ ในระบบ T-Reg (https://app.t-reg.co) จะใช้คำว่า ไม่มี และสัญลักษณ์ " – " หรือเมื่อ Export ไฟล์จะเป็นช่องว่างไว้.

12. การทำลายข้อมูลส่วนบุคคล

ให้ฝ่ายงานเจ้าของกิจกรรมที่ได้เก็บรวบรวมข้อมูลส่วนบุคคลพิจารณาดำเนินการทำลาย หรือทำให้เป็นข้อมูล นิรนามหลังจากครบระยะเวลาการจัดเก็บรักษาที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือครบระยะเวลาการจัดเก็บรักษาตามที่บริษัทฯ กำหนด หรือครบระยะเวลาการจัดเก็บรักษาตามที่กฎหมายกำหนดไว้ โดยการขออนุมัติทำลายข้อมูลจากผู้บริหารสายงานเจ้าของกิจกรรม

การพิจารณาทำลายข้อมูลส่วนบุคคลที่ได้เก็บรวบรวมไว้ให้ใช้ หลักเกณฑ์ดังต่อไปนี้

(1) เมื่อครบระยะเวลาการจัดเก็บรักษาที่ได้รับอนุญาตจากเจ้าของข้อมูลส่วนบุคคลตามที่ระบุไว้ในสัญญาหรือ ความยินยอม หรือครบระยะเวลาการจัดเก็บรักษาตามที่กฎหมายกำหนดไว้

(2) เมื่อข้อมูลส่วนบุคคลดังกล่าวหมดความจำเป็นในการจัดเก็บรักษาไว้ตามวัตถุประสงค์ของการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

(3) เมื่อพ้นกำหนดระยะเวลาการจัดเก็บรักษาข้อมูลส่วนบุคคลตามที่บริษัทฯ ได้กำหนดไว้และไม่มีข้อกำหนดทางกฎหมายใดระบุให้จัดเก็บรักษาเพิ่มเติม

(4) เมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอ หรือได้ถอนความยินยอม โดยบริษัทฯ ไม่มีอำนาจตามกฎหมายที่จะเก็บ รวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลนั้นได้ต่อไป

(5) เมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล โดยบริษัทฯ ไม่อาจปฏิเสธได้ตามเกณฑ์ที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

(6) เมื่อพบว่าข้อมูลส่วนบุคคลถูกเก็บรวบรวม ใช้หรือเปิดเผยโดยมิชอบด้วยกฎหมาย เมื่อมีการดำเนินการทำลายข้อมูลส่วนบุคคลให้ยึดหลักปฏิบัติของผู้มีหน้าที่ทำลายข้อมูล ดังนี้

(6.1) ให้ทำการตรวจสอบเป็นระยะ ๆ ทั้งนี้อาจเป็นรายเดือน รายไตรมาส หรือรายปีแล้วแต่ความเหมาะสม โดยให้มีการตรวจสอบระยะเวลาการจัดเก็บรักษาข้อมูลส่วนบุคคลว่าครบกำหนดที่ต้องถูกทำลายหรือไม่

(6.2) ให้จำกัดจำนวนผู้มีหน้าที่จัดการลบและทำลายข้อมูลให้มีจำนวนน้อยที่สุดเท่าที่จำเป็น

(6.3) ให้มีการบันทึกและทำรายงานสรุปผลการทำลายข้อมูล โดยมีรายละเอียด วัน เวลา สถานที่ เจ้าหน้าที่ผู้ดำเนินการ ผู้ควบคุม ลักษณะประเภทและจำนวนข้อมูลส่วนบุคคลที่ถูกทำลาย และวิธีที่ใช้ในการทำลาย เพื่อใช้ในการตรวจสอบและบริหารความเสี่ยงที่อาจเกิดขึ้นจากการรั่วไหลของข้อมูล

(6.4) ให้ยืนยันการทำลายข้อมูลส่วนบุคคลว่า ได้มีการทำลายจริงตามระยะเวลาการจัดเก็บรักษา

13. การประเมินความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล หมายถึง “ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรง หรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ”

บริษัทได้กำหนด “ข้อกำหนดการประเมินความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล” เพื่อใช้เป็นข้อกำหนดกลางของบริษัทฯ ในการประเมิน และบริหารจัดการความเสี่ยงของการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ ให้เป็นไปในทิศทางเดียวกัน โดยมุ่งเน้นการพิจารณาความเสี่ยงเฉพาะเรื่องการปฏิบัติการในการประมวลผลข้อมูล (Processing Operation) ครอบคลุมทั้งกระบวนการตั้งแต่การเก็บ (Collect) การเก็บรักษา (Storage) การใช้ (Use) การส่งต่อหรือเปิดเผย (Transfer) และการลบ หรือทำลาย (Disposal) ที่อาจจะทำให้เกิดการสูญหาย รั่วไหล หรือละเมิดข้อมูลส่วนบุคคล ซึ่งจะส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล การประเมินความเสี่ยงที่กำหนดนี้จะถูกนำไปใช้เป็นข้อมูลในการกำหนดมาตรการป้องกันคุ้มครองข้อมูลส่วนบุคคลที่เหมาะสมและเพียงพอที่จะทำให้สามารถลดความเสี่ยงของการละเมิดข้อมูลส่วนบุคคลลงต่ำที่สุด และมั่นใจว่าการคุ้มครองป้องกันข้อมูลส่วนบุคคลของบริษัทฯ เป็นไปอย่างมีประสิทธิภาพ เพียงพอ และเหมาะสม

(การละเมิดตามข้อกำหนดนี้ หมายถึง การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจ หรือโดยมิชอบ)

13.1 วัตถุประสงค์

13.1.1 เพื่อให้มั่นใจว่าการประเมิน และบริหารความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ จะเป็นไปในทิศทางเดียวกัน

13.1.2 เพื่อให้มั่นใจว่าการบริหารจัดการความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ เป็นไปอย่างเหมาะสม และมั่นใจว่าข้อมูลส่วนบุคคลจะได้รับความคุ้มครองตามที่กฎหมายกำหนด

13.2 ข้อกำหนดการบริหารจัดการความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล

บริษัทฯ ได้กำหนดหลักเกณฑ์การประเมิน และการบริหารจัดการความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล ดังนี้

13.2.1 คำนิยามที่เกี่ยวข้องกับการประเมินความเสี่ยงของการคุ้มครองข้อมูลส่วนบุคคล

1) ปัจจัยเสี่ยง (Risk Factor) คือ ต้นเหตุ หรือสาเหตุที่มาของความเสี่ยงที่จะทำให้เกิดการละเมิด หรือรั่วไหลของข้อมูลส่วนบุคคล ซึ่งเกิดได้จากทั้งปัจจัยภายในและภายนอกองค์กร
2) เหตุการณ์เสี่ยง คือ เหตุการณ์ที่ส่งผลกระทบต่อการดำเนินงาน
3) การประเมินระดับความรุนแรงของความเสี่ยง (Risk Assessment) เป็นการพิจารณาจากการประเมินระดับความรุนแรงทั้งโอกาสและผลกระทบของปัจจัยเสี่ยง ซึ่งประกอบด้วยโอกาสและความรุนแรงของผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล
   โดยระดับความรุนแรงของความเสี่ยง = โอกาสของการเกิดความเสี่ยง (Likelihood) X ระดับของผลกระทบ (Impact)
4) โอกาสที่จะเกิด (Likelihood) หมายถึง ความถี่ หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง
5) ผลกระทบ (Impact) หมายถึง ขนาดความรุนแรง (Severity) ที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลหากเกิดเหตุการณ์ความเสี่ยง
6) การตอบสนองความเสี่ยง (Risk Response) เป็นการพิจารณากำหนดแผนงาน หรือมาตรการที่จะตอบสนองต่อความเสี่ยงที่เกิดขึ้น
7) การบริหารความเสี่ยง (Risk Management) คือ กระบวนการที่ใช้ในการบริหารจัดการให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่บริษัทฯ ยอมรับได้
8) การติดตามผลและการประเมินผล (Monitoring) เป็นการพิจารณาจากการประเมินผลการควบคุมภายในของบริษัทฯ

13.2.2 ผู้รับผิดชอบการประเมิน และบริหารจัดการความเสี่ยง

1) ให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคล เป็นผู้ประเมินและวิเคราะห์ความเสี่ยงร่วมกับผู้ควบคุมข้อมูล เนื่องจากการวิเคราะห์ความเสี่ยงของข้อมูลส่วนบุคคลเป็นการวิเคราะห์เชิงเทคนิคมาก
2) ให้ผู้ควบคุมข้อมูลเป็นผู้รับผิดชอบในการบริหารจัดการความเสี่ยงในแต่ละปัจจัยเสี่ยงของข้อมูลส่วนบุคคลที่ตนเองรับผิดชอบ โดยอาจมอบหมายให้ผู้ประมวลผลร่วมดำเนินการด้วยก็ได้ และต้องรายงานผลการบริหารจัดการความเสี่ยงให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคล ทราบอย่างน้อยปีละ 1 ครั้ง

13.2.3 หลักเกณฑ์การประเมินความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล

การประเมินความเสี่ยง หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และการจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และความรุนแรงของผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล (Impact) จากเหตุการณ์ความเสี่ยงที่เกิดขึ้น

บริษัทฯ จึงได้กำหนดเกณฑ์มาตรฐานในการประเมินความเสี่ยง ทั้งโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) ออกเป็น 3 ระดับ เพื่อใช้เป็นเกณฑ์กลางในการประเมินความเสี่ยง ดังนี้

1) เกณฑ์มาตรฐานการประเมินระดับผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล (Impact)

บริษัทฯ ได้กำหนดเกณฑ์มาตรฐานกลางในการกำหนดระดับความรุนแรงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลที่เกิดจากการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลซึ่งเป็นการประเมินข้อมูลเชิงคุณภาพ โดยแบ่งออกเป็น 3 ระดับ ประกอบด้วย

ระดับผลกระทบ (Level of Impact)	นิยามผลกระทบ (Description)
ต่ำ	เจ้าของข้อมูลอาจมีความรู้สึกไม่สะดวก หรือรำคาญเพิ่มขึ้นเล็กน้อยในการที่เขาจะได้รับบริการหรือผลลัพธ์โดยปราศจากปัญหา (เช่น ระยะเวลาในการกรอกข้อมูลใหม่ การถูกรบกวน)
ปานกลาง	เจ้าของข้อมูลมีความรู้สึกไม่สะดวกอย่างมีนัยสำคัญ โดยยังสามารถได้รับบริการ หรือผลลัพธ์ถึงแม้จะมีความยากลำบากมากขึ้น (เช่น มีค่าใช้จ่ายเพิ่มเติม การปฏิเสธให้ได้รับการเข้าถึงการใช้บริการทางธุรกิจ ความกลัว ขาดความเข้าใจ ความเครียด)
สูง	เจ้าของข้อมูลพบความยากลำบาก หรือเสียหายมากอย่างมีนัยสำคัญ หรือรู้สึกว่าไม่คุ้มค่าในการรับบริการ หรือผลลัพธ์เมื่อเทียบกับความยากลำบากอย่างมากที่ได้รับ (เช่น ไม่เหมาะสมกับเงิน การถูกขึ้นบัญชีดำ ทรัพย์สินเสียหาย เลิกจ้าง สุขภาพเสียหาย ไม่สามารถทำงานได้ สูญเสียความสามารถทางกายภาพในระยะยาว)

2) เกณฑ์มาตรฐานการประเมินโอกาสที่จะเกิด (Likelihood)

บริษัทฯ ได้กำหนดเกณฑ์มาตรฐานกลางในการประเมินโอกาสที่จะเกิดการรั่วไหล หรือละเมิดข้อมูลส่วนบุคคลออกเป็น 3 ระดับ ประกอบด้วย

ระดับโอกาสที่จะเกิด (Level of Likelihood)	นิยามโอกาสที่จะเกิด (Description)
ต่ำ	โอกาสของภัยคุกคามนี้ต่ำมาก จนถึง ไม่น่าจะเกิดขึ้นได้ (มากกว่า 2 ปีต่อครั้ง)
ปานกลาง	มีโอกาสอย่างสมเหตุสมผลที่จะเกิดภัยคุกคามได้ (1 เดือน – 2 ปี ต่อครั้ง)
สูง	โอกาสของภัยคุกคามนี้ มีโอกาสบ่อยมาก พบได้ตลอดเวลา หรือสม่ำเสมอ (ต่ำกว่า 1 เดือนต่อครั้ง)

13.2.4 การประเมินความเสี่ยง (Risk Assessment)

บริษัทฯ ได้กำหนดการประเมินความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคล โดยมุ่งเน้นที่ผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล เพื่อนำไปใช้ในการออกแบบการป้องกันคุ้มครองข้อมูลส่วนบุคคล จึงได้แบ่งการประเมินความเสี่ยงการคุ้มครองข้อมูลส่วนบุคคลออกเป็น 2 กระบวนการ คือ

(ก) การประเมินความเสี่ยงความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล (Risk assessment of security of personal data processing) และ

(ข) การประเมินผลกระทบการคุ้มครองป้องกันข้อมูล (Data Protection Impact Assessment : DPIA) ที่จะทำในกรณีที่มีผลกระทบรุนแรงต่อสิทธิและเสรีภาพของเจ้าของข้อมูลและการลดความเสี่ยงนั้น

13.2.4.1 การประเมินความเสี่ยงความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล (Risk assessment of security of personal data processing) บริษัทได้กำหนดขั้นตอนการประเมินความเสี่ยงความปลอดภัยของการ ประมวลผลข้อมูลส่วนบุคคล และการบริหารความเสี่ยง ประกอบด้วย 2 ขั้นตอน ดังนี้

1) การกำหนดเกณฑ์มาตรฐานในการประเมินความเสี่ยง การกำหนดเกณฑ์ที่จะใช้ในการประเมินความเสี่ยง ได้แก่ ระดับโอกาส ที่จะเกิดความเสี่ยง (Likelihood) ระดับผลกระทบของความเสี่ยง (Impact) ซึ่งบริษัทได้กำหนดไว้ตาม ข้อ 13.2.3

2) การอธิบายรายละเอียดของการปฏิบัติการประมวลผล (Processing Operation) ขั้นตอนนี้เป็นการอธิบาย และแยกกระบวนการในการปฏิบัติการ ประมวลผลข้อมูลของแต่ละข้อมูล เพื่อจะได้นำกระบวนงานทั้งหมดมาพิจารณาหาความเสี่ยงที่จะเกิดขึ้นในกระบวนการทั้งหมด เช่น ชนิดของข้อมูลส่วนบุคคล วัตถุประสงค์ในการประมวลผล วิธีการในการใช้ข้อมูล ผู้รับข้อมูล เป็นต้น โดยมีตัวอย่าง ดังนี้

คำอธิบายการปฏิบัติการประมวลผลข้อมูล (Processing Operation Description)	**ระบุชื่อชุดข้อมูลส่วนบุคคล**
ข้อมูลส่วนบุคคลที่ดำเนินการ (Personal Data Processed)	ระบุข้อมูลส่วนบุคคลที่นำมาใช้ดำเนินการ เช่น ข้อมูลในการติดต่อ (ชื่อ สกุล ที่อยู่ เบอร์โทรศัพท์)
วัตถุประสงค์ของการประมวลผล (Processing Purpose)	ระบุ
เจ้าของข้อมูล (Data Subject)	ระบุ เช่น พนักงาน ลูกค้า ผู้รับจ้างเหมาบริการ (ฟรีแลนซ์)
วิธีการประมวลผล (Processing Means)	ระบุ วิธีการประมวลผลด้วยวิธีใด เช่น ผ่านระบบ Payroll
ผู้รับข้อมูล หรือผู้ที่ได้รับการเปิดเผยข้อมูล (Recipients of the Data)	ระบุ ภายในบริษัท คือใคร และภายนอกบริษัท คือใคร
ผู้ประมวลผลข้อมูล (Data Processor Used)	ระบุ

13.2.5 การประเมินระดับผลกระทบ (Impact)

การประเมินระดับผลกระทบเป็นการประเมินข้อมูลเชิงคุณภาพ โดยให้พิจารณาปัจจัยต่างๆ ตามที่มีอยู่ในการปฏิบัติการประมวลผลที่ระบุ เช่น ชนิดของข้อมูล จำนวนของข้อมูล จุดอ่อนไหวของการประมวลผล เป็นต้น มาประเมินผลกระทบว่าหากมีการสูญหาย รั่วไหล หรือละเมิดข้อมูลจะมีผลกระทบความรุนแรงต่อเจ้าของข้อมูลมากน้อยเพียงใด โดยการประเมินผลกระทบความรุนแรงของปัจจัยเสี่ยงแต่ละปัจจัยนี้ จะแบ่งมิติในการประเมินออกเป็น 3 มิติ คือ

(1) การสูญเสียการเป็นความลับ (Loss of Confidentiality)

(2) การสูญเสียความสมบูรณ์ถูกต้องของข้อมูล (Loss of Integrity)

(3) การสูญเสียในการเข้าถึงการใช้ข้อมูลได้ (Loss of Availability)

โดยให้พิจารณากำหนดระดับความรุนแรงของผลกระทบตามเกณฑ์มาตรฐานการประเมินระดับผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลตามที่กำหนดในข้อ 13.2.3 ทั้ง 3 มิติ ตามตารางตัวอย่างคำถามการประเมินระดับผลกระทบ ดังนี้

ลำดับ	คำถาม	ระดับการประเมินผลกระทบ
1	โปรดระบุระดับผลกระทบตามเกณฑ์มาตรฐานที่กำหนด หากเกิดการเปิดเผยข้อมูลจากผู้ไม่มีอำนาจ (สูญเสียการเป็นความลับ)	☐ ต่ำ ☐ ปานกลาง ☐ สูง
2	โปรดระบุระดับผลกระทบตามเกณฑ์มาตรฐานที่กำหนด หากเกิดการแก้ไขข้อมูลจากผู้ไม่มีอำนาจ (สูญเสียความสมบูรณ์ถูกต้องของข้อมูล)	☐ ต่ำ ☐ ปานกลาง ☐ สูง
3	โปรดระบุระดับผลกระทบตามเกณฑ์มาตรฐานที่กำหนด หากเกิดการทำลาย หรือลบข้อมูลจากผู้ไม่มีอำนาจ (สูญเสียการเข้าถึงการใช้ข้อมูลได้)	☐ ต่ำ ☐ ปานกลาง ☐ สูง

การพิจารณาว่าปัจจัยเสี่ยงใดมีผลกระทบความรุนแรงในระดับใด ให้นำผลการพิจารณาผลกระทบทั้ง 3 มิติข้างต้นมาพิจารณา โดยให้กำหนดระดับผลกระทบของปัจจัยเสี่ยงนั้น ตามระดับความรุนแรงสูงสุดจากที่พบในการประเมินทั้ง 3 มิติ เช่น

การประเมินผลกระทบความรุนแรง			
มิติการประเมิน	สูญเสียการเป็นความลับ (Confidentiality)	สูญเสียความสมบูรณ์ถูกต้องของข้อมูล (Integrity)	สูญเสียการเข้าถึงการใช้ข้อมูลได้ (Availability)
ผลการประเมิน	ปานกลาง	ต่ำ	ต่ำ
สรุปผลการประเมินผลกระทบความรุนแรงของปัจจัยเสี่ยงนี้		ปานกลาง	

13.2.6 การประเมินโอกาสที่จะเกิดขึ้น (Likelihood)

ขั้นตอนนี้เป็นขั้นตอนต่อเนื่องมาจากขั้นตอนที่แล้ว ในการประเมินถึงปัจจัยเสี่ยงต่าง ๆ หรือภัยคุกคามต่าง ๆ ที่จะเกิดขึ้นทั้งปัจจัยภายในบริษัทฯ และภายนอกบริษัทฯ นั้น นำมาประเมินโอกาสในการที่จะเกิดขึ้น เพื่อให้การประเมินโอกาสที่ภัยคุกคามนั้นจะเกิดขึ้น มีความง่ายและชัดเจนมากขึ้น จึงได้กำหนดมิติที่เกี่ยวข้องกับภัยคุกคามออกเป็น 4 มิติ ประกอบด้วย

(1) Network and technical resources (ทั้ง hardware และ software)

(2) กระบวนการและขั้นตอนที่เกี่ยวข้องกับการปฏิบัติการประมวลผล

(3) ความแตกต่างของคนที่เกี่ยวข้องกับการปฏิบัติการประมวลผล

(4) ธุรกิจและขนาดในการประมวลผลข้อมูล

โดยมีตัวอย่างคำถามที่ใช้ในการประเมินโอกาสที่ภัยคุกคามนั้นจะเกิดขึ้น

1. คำถามเกี่ยวกับ Network and technical resources

1.1	มีส่วนใดส่วนหนึ่งการประมวลผลที่ต้องดำเนินการผ่านระบบอินเตอร์เน็ตหรือไม่	การประมวลข้อมูลที่มีส่วนเกี่ยวข้องกับระบบอินเตอร์เน็ท จะมีโอกาสที่จะถูกคุกคามจากภายนอกสูงขึ้น โดยเฉพาะอย่างยิ่ง การให้บริการสำหรับผู้ใช้งานผ่านระบบอินเตอร์เน็ท

1.2	มีโอกาสในการยอมให้มีการเข้าถึงการประมวลผลข้อมูลส่วนบุคคลภายในบริษัทฯ จากระบบอินเตอร์เน็ทหรือไม่	เมื่อมีการยินยอมให้ทำการประมวลผลข้อมูลส่วนบุคคลภายในบริษัทฯ จากอินเตอร์เน็ต จะทำให้มีโอกาสที่ภัยคุกคามจะเกิดสูงขึ้น
1.3	ระบบประมวลผลข้อมูลส่วนบุคคลมีการเชื่อมโยงกับระบบสารสนเทศภายนอก หรือระบบอื่น ๆ ภายในบริษัทฯ หรือไม่	การเชื่อมโยงกับระบบสารสนเทศภายนอกบริษัทฯ จะทำให้โอกาสที่จะเกิดภัยคุกคามสูงขึ้น เช่นเดียวกับการเชื่อมโยงกับระบบอื่น ๆ ภายในบริษัทฯ ก็จะทำให้ผู้ไม่มีอำนาจมีโอกาสเข้าถึงข้อมูลสูงขึ้น
1.4	ผู้ไม่มีอำนาจอื่น ๆ สามารถเข้าถึงกระประมวลผลข้อมูลได้อย่างง่าย ๆ ใช่หรือไม่	การเปิดโอกาสให้ผู้ไม่มีอำนาจเข้าถึงการประมวลผลข้อมูลได้ง่ายๆ ทั้งระบบอิเล็กทรอนิกส์ หรือตู้จัดเก็บเอกสาร จะทำให้มีโอกาสเกิดภัยคุกคามสูงขึ้น
1.5	การออกแบบระบบการประมวลผลข้อมูล การดำเนินการ หรือบำรุงรักษาโดยไม่ได้พิจารณาจากแนวปฏิบัติที่ดีเลยใช่หรือไม่	การพิจารณาแนวปฏิบัติที่ดีแล้วนามาปรับใช้ จะทำให้โอกาสเกิดภัยคุกคามลดลง

2. คำถามเกี่ยวกับกระบวนการและขั้นตอนที่เกี่ยวข้องกับการปฏิบัติการประมวลผล

2.1	การกำหนดบทบาทและหน้าที่ความรับผิดชอบในกระบวนการประมวลผลข้อมูลมีความไม่ชัดเจนใช่หรือไม่	การที่ไม่มีการกำหนดบทบาทและหน้าที่ความรับผิดชอบที่ไม่ชัดเจน รวมถึงอำนาจในการเข้าถึงข้อมูลจะส่งผลให้ผู้ไม่มีอำนาจมีโอกาสในการเข้าถึงข้อมูลสูงขึ้น
2.2	การอนุญาตให้ใช้ระบบ เครือข่าย รวมถึงทรัพยากร มีความคลุมเครือ หรือไม่ชัดเจน ใช่หรือไม่	ความคลุมเครือ ไม่ชัดเจน จะทำให้มีโอกาสการใช้อย่างไม่เหมาะสม ซึ่งทำให้มีโอกาสเกิดภัยคุกคามสูงขึ้น การกำหนดนโยบายหรือแนวปฏิบัติจะช่วยลดความเสี่ยงต่ำลง
2.3	พนักงานได้รับอนุญาตในการนำ หรือใช้อุปกรณ์ส่วนตัวในการเชื่อมโยงเข้าถึงระบบการประมวลผลข้อมูลหรือไม่	การอนุญาตให้พนักงานใช้อุปกรณ์ส่วนตัวในการเข้าถึงระบบการประมวลผล จะทำให้มีโอกาสการเข้าถึงข้อมูลของผู้ไม่มีอำนาจสูงขึ้น และยังรวมถึงมีการนำไวรัส หรือ Bugs เข้าสู่ระบบง่ายยิ่งขึ้น
2.4	พนักงานได้รับอนุญาตให้ส่งต่อ หรือจัดเก็บข้อมูล ในการประมวลผลข้อมูลจากภายนอกบริษัทฯ	กระบวนการประมวลผลภายนอกบริษัทฯ จะเพิ่มโอกาสของภัยคุกคามมากยิ่งขึ้น เช่น การใช้ WIFI ของภายนอกบริษัทฯ
2.5	กิจกรรมในการประมวลผลที่จะส่งต่อ หรือนำออกไปภายนอก มีการกำหนด log files ไว้หรือไม่	การขาดการจัดเก็บข้อมูล และการติดตามที่เหมาะสมจะส่งผลให้โอกาสในการละเมิดข้อมูลสูงขึ้น

3. คำถามเกี่ยวกับความแตกต่างของบุคคลที่เกี่ยวข้องกับการปฏิบัติการประมวลผล

3.1	การประมวลผลข้อมูลส่วนบุคคลโดยไม่ได้ระบุจำนวนพนักงานที่ดำเนินการใช่หรือไม่	การประมวลผลข้อมูลที่เปิดกว้าง หรือมีจำนวนพนักงานที่เข้าร่วมประมวลผลจำนวนมาก จะทำให้มีโอกาสการละเมิดข้อมูลสูงขึ้น
3.2	มีกระบวนการ หรือขั้นตอนในการประมวลผลข้อมูลส่วนบุคคลใดที่ให้ที่ปรึกษา หรือบุคคลภายนอกที่ 3 เข้ามาเป็นผู้ประมวลผลข้อมูลหรือไม่	การประมวลผลข้อมูลจากที่ปรึกษา หรือบุคคลที่ 3 ภายนอกบริษัทฯ จะทำให้การควบคุมเป็นไปได้ยากขึ้น ก็ทำให้มีโอกาสเกิดภัยคุกคามมากยิ่งขึ้น
3.3	มีข้อกำหนดให้บุคคลที่เกี่ยวข้องกับการปฏิบัติการประมวลผลข้อมูลที่คลุมเครือ ไม่ชัดเจนหรือไม่	ถ้าข้อกำหนดใด ๆ ในการปฏิบัติไม่ชัดเจน ก็จะส่งผลให้ผู้ปฏิบัติอาจดำเนินการใช้ที่ไม่ถูกต้อง เช่น การลบ หรือทำลาย ซึ่งจะทำให้โอกาสเกิดภัยคุกคามสูงขึ้น

3.4	บุคคลที่เกี่ยวข้องกับการปฏิบัติการประมวลผลข้อมูลที่ไม่คุ้นชินกับระบบการป้องกันความมั่นคงปลอดภัยของระบบสารสนเทศหรือไม่	บุคคลที่ไม่ได้ตระหนักถึงจำเป็นของมาตรการทางด้านการป้องกันความมั่นคงปลอดภัย ก็จะทำให้มีโอกาสความเสี่ยงที่จะทำให้ข้อมูลรั่วไหล หรือละเมิดเพิ่มสูงขึ้น
3.5	มีบุคคลที่เกี่ยวข้องกับการปฏิบัติการประมวลผลข้อมูลมีการละเลยการเก็บรักษาข้อมูลอย่างปลอดภัยหรือการทำลายข้อมูลส่วนบุคคลหรือไม่	การละเมิดข้อมูลส่วนบุคคลหลายครั้งเกิดจากการละเลยในการดูแลที่จัดเก็บเอกสารที่ดีเพียงพอ

4. คำถามเกี่ยวกับธุรกิจและขนาดในการประมวลผลข้อมูล

4.1	ธุรกิจของบริษัทฯ เป็นธุรกิจที่มักจะโดนหรือน่าสนใจที่จะโจมตี หรือโจรกรรมข้อมูลทางอิเล็กทรอนิกส์หรือไม่	เมื่อการโจรกรรมข้อมูลมักจะมีการโจมตี หรือโจรกรรมในธุรกิจบางธุรกิจ หากธุรกิจของบริษัทฯ อยู่ในกลุ่มเหล่านั้นก็จะทำให้มีโอกาสในการเกิดภัยคุกคามสูงขึ้น
4.2	บริษัทฯ มีการถูกโจมตี หรือโจรกรรมข้อมูล หรือการละเมิดข้อมูลอื่นใดในรอบ 2 ปีหรือไม่	บริษัทฯ ที่เคยโดนโจมตี หรือโจรกรมข้อมูล รวมถึงการละเมิดข้อมูลอื่นใด ย่อมมีโอกาสที่จะถูกกระทำซ้ำอีก หากไม่มีมาตรการมารองรับและแก้ไขไว้
4.3	บริษัทฯ ได้รับการแจ้งเตือน หรือร้องเรียนเกี่ยวกับระบบความมั่นคงปลอดภัยด้าน IT ภายใน 1 ปีหรือไม่	การได้รับการแจ้งเตือน หรือเรื่องร้องเรียนจะเป็นตัวบ่งชี้ถึงความเข้มแข็งของระบบการป้องกันความมั่นคงปลอดภัย
4.4	การประมวลผลข้อมูลมีการประมวลผลข้อมูลส่วนบุคคลจำนวนมาก ๆ หรือไม่	จำนวนข้อมูลจะเป็นสิ่งดึงดูดให้นักโจมตี หรือโจรกรรมข้อมูลเข้ามาโจมตี หรือโจรกรรมข้อมูลสูงยิ่งขึ้น
4.5	มีระบบการป้องกันความมั่นคงปลอดภัยที่เป็นแนวปฏิบัติที่ดีให้บริษัทฯ ได้พิจารณาความเหมาะสมในการปฏิบัติตามหรือไม่	ธุรกิจเฉพาะบางธุรกิจมีความจำเป็นต้องมีระบบการป้องกันความมั่นคงปลอดภัยโดยเฉพาะหรือไม่

การพิจารณาว่าปัจจัยเสี่ยงใดมีโอกาสเกิดภัยคุกคามในระดับใด ให้ดำเนินการประเมินโอกาสในการเกิดภัยคุกคามทั้ง 4 มิติ ตามตารางข้างล่างนี้

มิติในการประเมิน	**โอกาสที่จะเกิดภัยคุกคาม**	
	ระดับ	**คะแนน**
Network and technical resources	ต่ำ	1
	ปานกลาง	2
	สูง	3
กระบวนการและขั้นตอนที่เกี่ยวข้องกับการปฏิบัติการประมวลผล	ต่ำ	1
	ปานกลาง	2
	สูง	3
ความแตกต่างของบุคคลที่เกี่ยวข้องกับการปฏิบัติการประมวลผล	ต่ำ	1
	ปานกลาง	2
	สูง	3
ธุรกิจและขนาดในการประมวลผลข้อมูล	ต่ำ	1
	ปานกลาง	2
	สูง	3

ปัจจัยเสี่ยงใดจะมีโอกาสเกิดภัยคุกคามระดับใดตามเกณฑ์มาตรฐานที่กำหนด จะเป็นไปตามตารางนี้

คะแนนรวมของโอกาสที่จะเกิดภัยคุกคาม	ระดับโอกาสเกิดภัยคุกคาม
4-5	ต่ำ
6-8	ปานกลาง
9-12	สูง

13.2.7 การประเมินและจัดลำดับความเสี่ยง

เมื่อได้ค่าระดับผลกระทบ (Impact) และโอกาสที่จะเกิดขึ้น (Likelihood) จากการพิจารณาในข้อ 13.3 และ 13.4 แล้ว ให้นำมาประเมินและจัดลำดับความรุนแรงของความเสี่ยงที่มีผลกระทบต่อบริษัทฯ เพื่อพิจารณากำหนดกิจกรรมการบริหารจัดการความเสี่ยงและควบคุมในแต่ละสาเหตุของความเสี่ยงที่สำคัญให้เหมาะสมตามลำดับความรุนแรงของความเสี่ยง โดยบริษัทฯ ได้กำหนดระดับความรุนแรงของความเสี่ยง ออกเป็น 3 ระดับ คือ

(1) ระดับความเสี่ยง**ต่ำ** ตาม**ช่องสีเขียว**

(2) ระดับความเสี่ยง**ปานกลาง** ตาม**ช่องสีเหลือง**

(3) ระดับความเสี่ยง**สูง** ตาม**ช่องสีแดง**

ตามตารางการวิเคราะห์ความเสี่ยงและระดับความรุนแรงของความเสี่ยงนี้

ระดับผลกระทบ (Impact)	**สูง**			
	ปานกลาง			
	ต่ำ			
ระดับโอกาสที่จะเกิดขึ้น (Likelihood)		**ต่ำ**	**ปานกลาง**	**สูง**

บริษัทฯ ได้กำหนดขอบเขตของความรุนแรงที่องค์กรยอมรับได้ (Risk Boundary/ Risk Tolerance) อยู่ที่ระดับความเสี่ยง**ต่ำ**

13.3 การกำหนดการตอบสนองความเสี่ยง และแผนบริหารจัดการความเสี่ยง

ให้ผู้ควบคุมข้อมูลเป็นผู้รับผิดชอบกำหนดแนวทางในการตอบสนองความเสี่ยงในแต่ละปัจจัยเสี่ยงของข้อมูลส่วนบุคคลที่ตนเองรับผิดชอบที่เกิดขึ้น พร้อมกับกำหนดแผนงานในการบริหารจัดการความเสี่ยงให้มีโอกาสต่ำลง หรือมีผลกระทบที่ต่ำลง พร้อมทั้งดำเนินการให้เป็นไปตามแผนงานที่กำหนด

ผู้รับผิดชอบดำเนินการบริหารจัดการความเสี่ยง ต้องพิจารณาและดำเนินการให้ปัจจัยเสี่ยงทั้งหมดจะต้องไม่อยู่ในระดับสูง

13.4 การติดตามและประเมินผล

ให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคล เป็นผู้ติดตาม และประเมินการบริหารจัดการความเสี่ยงตามแผนบริหารจัดการความเสี่ยงที่กำหนดและรายงานให้คณะกรรมการบริหารความเสี่ยงรับทราบในการประชุมคณะกรรมการบริหารความเสี่ยง

13.4.1 การประเมินผลกระทบการคุ้มครองป้องกันข้อมูล(Data Protection Impact Assessment : DPIA)

บริษัทฯ ได้กำหนดให้งาน หรือโครงการใด ๆ รวมถึงการทำโครงการใหม่ที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลที่มีการประเมินว่ามีโอกาสที่จะมีความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล จะต้องถูกนำมาประเมินผลกระทบการคุ้มครองข้อมูล (DPIA) และนำไปบริหารจัดการเพื่อลดความเสี่ยงที่จะเกิดขึ้น รวมถึงเมื่อพบว่ามีการละเมิดข้อมูลส่วนบุคคล จะต้องทำการประเมินผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลว่าได้รับผลกระทบรุนแรงหรือไม่

1) การประมวลผลข้อมูลที่มีการประเมินว่ามีโอกาสที่จะมีความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล การประมวลผลข้อมูลส่วนบุคคลใดที่มีโอกาสสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล หรือการประมวลผลข้อมูลส่วนบุคคลที่มีผลกระทบรุนแรง (สูง) ต่อสิทธิและเสรีภาพของเจ้าของข้อมูล ถือว่าเป็นการประมวลผลข้อมูลส่วนบุคคลที่มีการประเมินว่ามีโอกาสที่จะมีความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลจำเป็นต้องดำเนินการประเมินผลกระทบการคุ้มครองข้อมูล (DPIA) โดยการกำหนดเกณฑ์โอกาส และผลกระทบให้เป็นไปตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด แต่หากไม่มีการกำหนดให้ใช้เกณฑ์มาตรฐานที่บริษัทฯ กำหนดไว้ตามข้อ 13.2.3 โดยอนุโลม

การประมวลผลข้อมูลส่วนบุคคลที่เป็นการประมวลผลที่มีโอกาสความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล และต้องดำเนินการจัดทำ DPIA ประกอบด้วย

(1) การประมวลผลข้อมูลส่วนบุคคลอย่างกว้างขวางด้วยระบบอัตโนมัติ (Systematic and extensive profiling with significant effects) รวมถึงการทำโปรไฟลิ่ง (Profiling) ซึ่งการประมวลผลดังกล่าวส่งผลต่อการตัดสินใจที่ส่งผลทางกฎหมาย หรือส่งผลที่มีนัยสำคัญทำนองเดียวกันต่อบุคคล

(2) การประมวลผลข้อมูลจำนวนมากที่เป็นข้อมูลที่อ่อนไหว (Processing of sensitive data on a large scale) เช่น ข้อมูลอาชญากรรม

(3) การตรวจตราและเฝ้าดูพื้นที่สาธารณะขนาดใหญ่ (Public monitoring on a large scale) เช่น ศูนย์การค้า ห้องประชุม ถนนและตรอกซอกซอย ตลาด สถานีรถไฟ หรือห้องสมุดสาธารณะ เป็นต้น

นอกจากนี้ ในกรณีที่มีการวางแผนที่จะทำโครงการที่มีการประมวลผลข้อมูลส่วนบุคคลเกี่ยวข้องกับข้อมูลเหล่านี้ควรต้องจัดทำ DPIA ประกอบด้วย

(4) การใช้เทคโนโลยีที่เป็นนวัตกรรมใหม่

(5) การทำโปรไฟลิ่งในประเภทที่เป็นธุรกิจเฉพาะ

(6) การทำโปรไฟล์ของข้อมูลส่วนบุคคลขนาดใหญ่

(7) การติดตามพฤติกรรม หรือสถานที่ของบุคคล

(8) การทำโปรไฟล์ข้อมูลเด็ก

(9) การประมวลผลข้อมูลที่อาจทำให้เกิดภัยต่อร่างกายของบุคคล เป็นต้น

บริษัทฯ ได้ทำการประเมินกิจกรรมของบริษัทฯ ที่มีโอกาสความเสี่ยงสูงที่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูล และต้องดำเนินการจัดทำ DPIA **ตามหลักเกณฑ์ข้างต้น ไม่พบว่า บริษัทฯ มีกิจกรรมการประมวลผลข้อมูลใดที่จะเข้าหลักเกณฑ์ดังกล่าว จึงไม่มีความจำเป็นต้องทำ DPIA**

14. การปกป้องข้อมูลส่วนบุคคล

บริษัทฯ จะใช้มาตรการทางเทคนิค และการบริหารจัดการที่เหมาะสมเพื่อป้องกันและรักษาความปลอดภัยของข้อมูลส่วนบุคคลของท่าน โดยมีการเข้ารหัสสำหรับการส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ตและควบคุมการเข้าถึงข้อมูลส่วนบุคคลของท่านเฉพาะผู้เกี่ยวข้อง ทั้งในส่วนของข้อมูลที่จัดเก็บในรูปแบบเอกสารและอิเล็กทรอนิกส์

15. การเชื่อมต่อเว็บไซต์ หรือบริการภายนอก

บริการของบริษัทฯ อาจมีการเชื่อมต่อไปยังเว็บไซต์ หรือบริการของบุคคลที่สาม ซึ่งเว็บไซต์ หรือบริการดังกล่าวอาจมีการประกาศนโยบายการคุ้มครองข้อมูลส่วนบุคคลที่มีเนื้อหาสาระแตกต่างจากนโยบายนี้ บริษัทฯ ขอแนะนำให้ท่านศึกษานโยบายการคุ้มครองข้อมูลส่วนบุคคลของเว็บไซต์ หรือบริการนั้น ๆ เพื่อทราบในรายละเอียดก่อนการเข้าใช้งาน ทั้งนี้ บริษัทฯ ไม่มีความเกี่ยวข้องและไม่มีอำนาจควบคุมถึงมาตรการคุ้มครองข้อมูลส่วนบุคคลของเว็บไซต์ หรือบริการดังกล่าวและไม่สามารถรับผิดชอบต่อเนื้อหานโยบาย ความเสียหาย หรือการกระทำอันเกิดจากเว็บไซต์ หรือบริการของบุคคลที่สาม

16. คณะทำงานคุ้มครองข้อมูลส่วนบุคคล

บริษัทฯ ได้แต่งตั้งคณะทำงานคุ้มครองข้อมูลส่วนบุคคลเพื่อทำหน้าที่ตรวจสอบ กำกับและให้คำแนะนำในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงการประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เพื่อให้สอดคล้องตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

17. สิทธิของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

ท่านสามารถขอใช้สิทธิต่าง ๆ ตามที่กฎหมายกำหนด และตามที่ระบุไว้ในประกาศฉบับนี้ ได้ดังต่อไปนี้

1. สิทธิในการขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคล
2. สิทธิในการขอแก้ไขข้อมูลดังกล่าวให้เป็นปัจจุบันและถูกต้อง
3. สิทธิในการขอรับข้อมูลส่วนบุคคล ในกรณีที่บริษัทฯ ได้ทำให้ข้อมูลส่วนบุคคลนั้นอยู่ในรูปแบบที่สามารถอ่าน หรือใช้งานโดยทั่วไปได้ด้วยเครื่องมือ หรืออุปกรณ์ที่ทำงานได้โดยอัตโนมัติและสามารถใช้ หรือเปิดเผยข้อมูลส่วนบุคคลได้ด้วยวิธีการอัตโนมัติ
4. สิทธิในการขอลบ หรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลได้ เมื่อข้อมูลนั้นหมดความจำเป็น หรือเมื่อเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม
5. สิทธิในการขอระงับการใช้ข้อมูลส่วนบุคคล ในกรณีเมื่อเป็นข้อมูลส่วนบุคคลที่ต้องลบ หรือเมื่อข้อมูลดังกล่าวหมดความจำเป็น
6. สิทธิในการถอนความยินยอมในการประมวลผลข้อมูลที่ผู้ใช้บริการเคยให้ไว้
7. สิทธิในการขอคัดค้าน เจ้าของข้อมูลส่วนบุคคลมีสิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลเมื่อใดก็ได้

18. โทษของการไม่ปฏิบัติตามนโยบายการคุ้มครองข้อมูลส่วนบุคคล

การไม่ปฏิบัติตามนโยบายอาจมีผลเป็นความผิดและถูกลงโทษทางวินัยตามกฎเกณฑ์ของบริษัทฯ (สำหรับเจ้าหน้าที่ หรือผู้ปฏิบัติงานของบริษัทฯ) หรือตามข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (สำหรับผู้ประมวลผลข้อมูลส่วนบุคคล) ทั้งนี้ ตามแต่กรณีและความสัมพันธ์ที่ท่านมีต่อบริษัทฯ และอาจได้รับโทษตามที่กำหนดโดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 รวมทั้งกฎหมายลำดับรอง กฎ ระเบียบ คำสั่งที่เกี่ยวข้อง

19. การร้องเรียนต่อหน่วยงานผู้มีอำนาจกำกับดูแล

ในกรณีที่ท่านพบว่า บริษัทฯ มิได้ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ท่านมีสิทธิร้องเรียนไปยังคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือหน่วยงานที่มีอำนาจกำกับดูแลที่ได้รับการแต่งตั้ง โดยคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล หรือตามกฎหมายทั้งนี้ ก่อนการร้องเรียนดังกล่าว บริษัทฯ ขอให้ท่านโปรดติดต่อมายังบริษัทฯ เพื่อให้บริษัทฯ มีโอกาสได้รับทราบข้อเท็จจริงและได้ชี้แจงในประเด็นต่าง ๆ รวมถึงจัดการแก้ไขข้อกังวลของท่านก่อนในโอกาสแรก

20. การปรับปรุงแก้ไขนโยบายการคุ้มครองข้อมูลส่วนบุคคล

บริษัทฯ อาจพิจารณาปรับปรุง แก้ไข หรือเปลี่ยนแปลงนโยบายนี้ตามที่เห็นสมควร และจะทำการแจ้งให้ท่านทราบผ่านช่องทางเว็บไซต์ เช่น https://www.nbd.co.th/th โดยมีวันที่มีผลบังคับใช้ของแต่ละฉบับแก้ไขกำกับอยู่ อย่างไรก็ดี บริษัทฯ ขอแนะนำให้ท่านโปรดตรวจสอบเพื่อรับทราบนโยบายฉบับใหม่อย่างสม่ำเสมอ ผ่านช่องทางเฉพาะกิจกรรมที่บริษัทฯ ดำเนินการ โดยเฉพาะก่อนที่ท่านจะทำการเปิดเผยข้อมูลส่วนบุคคลแก่ บริษัทฯ

การเข้าใช้งานผลิตภัณฑ์ หรือบริการของบริษัทฯ ภายหลังการบังคับใช้นโยบายใหม่ ถือเป็นการรับทราบตามข้อตกลงในนโยบายใหม่แล้ว ทั้งนี้ โปรดหยุดการเข้าใช้งานหากท่านไม่เห็นด้วยกับรายละเอียดในนโยบายฉบับนี้และโปรดติดต่อมายังบริษัทฯ เพื่อชี้แจงข้อเท็จจริงต่อไป

21. การติดต่อสอบถามหรือใช้สิทธิ

หากท่านมีข้อสงสัย ข้อเสนอแนะ หรือข้อกังวลเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลของบริษัทฯ หรือเกี่ยวกับนโยบายนี้ หรือท่านต้องการใช้สิทธิตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล ท่านสามารถติดต่อสอบถามได้ที่

ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)

บริษัท เอ็นบีดี เฮลท์แคร์ จำกัด

เลขที่ 898 ซอยนวลจันทร์ 56 แขวงนวลจันทร์ เขตบึงกุ่ม กรุงเทพมหานคร 10230

โทรศัพท์ : (+66)2 791 3888 ต่อ 1160

โทรสาร : (+66)2 791 3716

อีเมล : dpo@nbd.co.th

คณะทำงานคุ้มครองข้อมูลส่วนบุคคล

บริษัท เอ็นบีดี เฮลท์แคร์ จำกัด และบริษัทย่อย

เลขที่ 898 ซอยนวลจันทร์ 56 แขวงนวลจันทร์ เขตบึงกุ่ม กรุงเทพมหานคร 10230

โทรศัพท์ : (+66)2 791 3888 ต่อ 1160

โทรสาร : (+66)2 791 3716

อีเมล : dpo@nbd.co.th

โดยแจ้งข้อมูลดังต่อไปนี้ประกอบการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคล

- ชื่อ นามสกุล เลขที่บัตรประจำตัวประชาชน/เลขที่หนังสือเดินทาง
- ข้อสงสัยเกี่ยวกับข้อมูลส่วนบุคคล หรือสิทธิที่ต้องการใช้ตามกฎหมาย
- หมายเลขโทรศัพท์ ที่อยู่ และอีเมลที่สามารถติดต่อกลับได้

ทั้งนี้ นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) บริษัท เอ็นบีดี เฮลท์แคร์ จำกัด และบริษัทย่อย ฉบับนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ 5 เมษายน พ.ศ.2566 เป็นต้นไป หรือจนกว่าจะมีการเปลี่ยนแปลง

ประกาศ ณ วันที่ 5 เมษายน พ.ศ.2566

(นายสุวิทย์ เมษินทรีย์)

ประธานกรรมการบริษัท