ต้นฉบับ

บริษัท เอส.เอ.เอฟ. สเปเชียล สตีล จำกัด (มหาชน)

S.A.F. SPECIAL STEEL PUBLIC COMPANY LIMITED

ระเบียบปฏิบัติงาน

(Standard Procedure)

เรื่อง การคุ้มครองข้อมูลส่วนบุคคล

(เลขที่ SP-MG-01)

แก้ไขครั้งที่ 01 ประกาศใช้วันที่ 18 ธันวาคม 2568

จัดทำโดย	สอบทานโดย	อนุมัติโดย
(ภญ. ลีนา อริยเดชวณิช) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	(นายพิศาล อริยเดชวณิช) ประธานเจ้าหน้าที่ฝ่ายปฏิบัติการ	(ดร.พิศิษฐ์ อริยเดชวณิช) ประธานเจ้าหน้าที่บริหาร

ประวัติการจัดทำ และทบทวนเอกสาร

ครั้งที่	วันที่แก้ไข	รายละเอียด
00	22 ก.ค. 65	เผยแพร่เพื่อใช้งานครั้งที่ 1
01	18 ธ.ค. 68	ทบทวนแก้ไขให้เหมาะสมสอดคล้องกับนโยบายคุ้มครองข้อมูลส่วนบุคคล

1. วัตถุประสงค์

1.1 เพื่อให้การทำธุรกรรมกับบริษัท เอส.เอ.เอฟ. สเปเชียล สตีล จำกัด (มหาชน) มีความมั่นคงปลอดภัย น่าเชื่อถือ คุ้มครองข้อมูลส่วนบุคคลของบุคลากร ลูกค้า คู่ค้าธุรกิจ และพันธมิตรทางธุรกิจทั้งหมด

1.2 เพื่อป้องกันความเสียหายที่เกิดจากการนำข้อมูลส่วนบุคคลไปแสวงหาประโยชน์โดยทุจริตหรือนำไปใช้ในทางที่ผิด

2. ขอบเขต

เพื่อใช้เป็นแนวทางปฏิบัติงานในการคุ้มครองข้อมูลส่วนบุคคลของบริษัท พนักงานบริษัท ตลอดจนบุคคลที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งของบริษัท หรือกระทำการดังกล่าวในนามบริษัท โดยครอบคลุมการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของ ลูกค้า พนักงาน ผู้ถือหุ้น

คู่ค้า และบุคคลต่าง ๆ ที่เกี่ยวข้องกับการให้บริการของบริษัทหรือทำธุรกรรมกับบริษัท

คำนิยาม

PDPA (Personal Data Protection Act) หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งกำหนดให้องค์กรในประเทศไทย รวมถึงบริษัทหลักทรัพย์ เก็บรวบรวม ประมวลผลและคุ้มครองข้อมูลส่วนบุคคล ด้วยมาตรการรักษาความปลอดภัยที่เหมาะสม

“คณะกรรมการ (Board of Directors)” หมายถึง คณะกรรมการของบริษัท เอส.เอ.เอฟ. สเปเชียล สตีล จำกัด (มหาชน)

“ผู้บริหาร (Management)” หมายถึง ผู้บริหารของบริษัท เอส.เอ.เอฟ. สเปเชียล สตีล จำกัด (มหาชน)

“พนักงาน (Staff)” หมายถึง พนักงานในระดับรองลงมาจากระดับผู้บริหารของ บริษัท เอส.เอ.เอฟ. สเปเชียล-สตีล จำกัด (มหาชน)

"ข้อมูลส่วนบุคคล (Personal Data)" หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวตนบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ เช่น ชื่อ นามสกุล หมายเลขโทรศัพท์ ที่อยู่ หมายเลขบัตรประจำตัวประชาชน ข้อมูลอื่นๆ อาทิ พฤติกรรมการเยี่ยมชมเว็บไซต์ของบริษัท ภาพถ่ายจากกล้องวงจรปิด บันทึกภาพและเสียง บันทึกเสียงการสนทนา หรือหมายเลข IP Address ของคอมพิวเตอร์ เป็นต้น เป็นต้น

"ข้อมูลส่วนบุคคลที่ละเอียดอ่อน / ข้อมูลส่วนบุคคลอ่อนไหว (Sensitive Personal Data)" หมายถึง ข้อมูลตามมาตรา 26 แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งรวมถึงแต่ไม่จำกัดเพียง เชื้อชาติ ศาสนา ข้อมูลชีวภาพ (Biometrics) ข้อมูลเกี่ยวกับสุขภาพ ประวัติอาชญากรรม ข้อมูลความเห็นทางการเมือง พฤติกรรมทางเพศ หรือข้อมูลสหภาพแรงงาน เป็นต้น เป็นข้อมูลที่เป็นเรื่องส่วนบุคคลโดยแท้ของบุคคล แต่มีความละเอียดและอาจสุ่มเสี่ยงในการเลือกปฏิบัติอย่างไม่เป็นธรรม เช่น เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

"ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)" หมายถึง บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

"ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)" หมายถึง บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของบริษัท ทั้งนี้ บุคคลหรือนิติบุคคล ซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

"เจ้าของข้อมูลส่วนบุคคล (Data Subject)" หมายถึง บุคคลธรรมดาซึ่งเป็นเจ้าของข้อมูลส่วนบุคคลที่ข้อมูลส่วนบุคคลสามารถระบุตัวตนของบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม

"การประมวลผล" หมายถึง การดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ เปิดเผย การลบ หรือการทำลายข้อมูลส่วนบุคคล

"บุคคลภายนอก หรือ บริษัทภายนอก (Third parties)" หมายถึง บุคคลหรือนิติบุคคลนอกเหนือจากเจ้าของข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลข้อมูลส่วนบุคคลที่ได้รับจ้างให้ประมวลข้อมูลในนามบริษัท เอส.เอ.เอฟ. สเปเชียล สตีล จำกัด (มหาชน)

"เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO)" หมายถึง บุคคลที่ถูกแต่งตั้ง ให้มีหน้าที่ให้คำแนะนำ และตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคล ให้ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

"ประกาศความเป็นส่วนตัว (Privacy Notice)" หมายถึง การประกาศบนเว็บไซต์เพื่อแจ้งผู้เข้ามาใช้เว็บไซต์ถึงจุดประสงค์ วิธีการรวบรวม ประมวล และจัดเก็บข้อมูลส่วนบุคคลของเว็บไซต์

"คุกกี้ (Cookies)" หมายถึง ไฟล์เป็นเอกลักษณ์ซึ่งสร้างโดยเว็บไซต์และจัดเก็บบนคอมพิวเตอร์ หรืออุปกรณ์สื่อสารของผู้ใช้งานซึ่งจะจัดเก็บข้อมูลส่วนบุคคล การใช้งาน และการตั้งค่าต่าง ๆ ของผู้ใช้งานเพื่อปรับปรุงประสบการณ์ใช้งานเว็บไซต์ของผู้ใช้งาน

3. หน่วยงานที่เกี่ยวข้อง

- แผนกทรัพยากรบุคคล
- แผนกจัดหา
- ส่วนขายและการตลาด (ประกอบด้วยแผนกประสานงานขาย และแผนกขาย)
- ส่วนบัญชีและส่วนการเงิน
- แผนกเทคโนโลยีสารสนเทศ
- ทุกหน่วยงานที่มีการใช้ หรือเกี่ยวข้องกับการเก็บรวบรวมข้อมูลส่วนบุคคล

4. นโยบายและหลักการ

การคุ้มครองข้อมูลส่วนบุคคลฉบับนี้ มีผลบังคับใช้กับลูกค้า พนักงาน ผู้ถือหุ้น คู่ค้า และบุคคลต่าง ๆ ที่เกี่ยวข้องกับการให้บริการของบริษัทหรือทำธุรกรรมกับบริษัท

4.1 การควบคุมข้อมูลส่วนบุคคล

บริษัท เอส.เอ.เอฟ. สเปเชียล สตีล จำกัด (มหาชน) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการตามหลักการคุ้มครองข้อมูลส่วนบุคคลตามที่ระบุด้านล่างนี้ เพื่อให้เกิดการใช้ข้อมูลส่วนบุคคลอย่างถูกต้อง บริษัท เอส.เอ.เอฟ. สเปเชียล สตีล จำกัด (มหาชน) ต้องจัดการให้มีการปฏิบัติดังต่อไปนี้

1) แจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบวัตถุประสงค์ เงื่อนไขและขอความยินยอม (ถ้ามี) ก่อนการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
2) เก็บ รวบรวม ใช้ และเปิดเผย ข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์ที่ได้แจ้งแก่เจ้าของข้อมูลส่วนบุคคล
3) ป้องกันไม่ให้มีการนำข้อมูลไปใช้หรือเปิดเผยโดยไม่ได้รับอนุญาต
4) จัดให้มีมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลในการจัดเก็บ ใช้ หรือเปิดเผย รวมถึงการส่งหรือโอนข้อมูลส่วนบุคคลไปยังบุคคลอื่นและต้องมีการทบทวนมาตรการให้สอดคล้องกับการเปลี่ยนแปลง
5) แก้ไข เปลี่ยนแปลง ลบ หรือทำลายข้อมูลตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ
6) จัดให้มีการติดตาม ตรวจสอบการลบหรือทำลายข้อมูลส่วนบุคคล เมื่อการเก็บข้อมูลเกินกำหนดระยะเวลา ข้อมูลที่ไม่เกี่ยวข้อง หรือเกินความจำเป็นตามวัตถุประสงค์ที่ได้ระบุไว้ เจ้าของข้อมูลร้องขอ หรือถอนความยินยอม
7) จัดให้มีการกำหนดสิทธิและข้อจำกัดสิทธิในการเข้าถึงข้อมูลส่วนบุคคล
8) จัดให้มีการบันทึกรายการข้อมูลส่วนบุคคล เพื่อให้เจ้าของข้อมูลส่วนบุคคลสามารถเข้าถึงหรือตรวจสอบได้
9) แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลทันทีเมื่อตรวจพบ

4.2 การประมวลผลข้อมูลส่วนบุคคล

ในการประมวลผลข้อมูลส่วนบุคคล บริษัท เอส.เอ.เอฟ. สเปเชียล สตีล จำกัด (มหาชน) จัดให้มีการดำเนินการเพื่อป้องกันการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผยโดยผิดกฎหมายหรือปราศจากการให้

ความยินยอม โดยให้ผู้ประมวลข้อมูลให้บริษัท เอส.เอ.เอฟ. สเปเชียล สตีล จำกัด (มหาชน) ซึ่งรวมทั้งบุคคลภายใน บุคคลภายนอก และนิติบุคคลภายนอก ดำเนินการดังต่อไปนี้

1) ดำเนินการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามที่ได้รับคำสั่งจากผู้ควบคุมข้อมูลส่วนบุคคล
2) จัดให้มีมาตรการรักษาความปลอดภัย เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล
3) บันทึกและเก็บรักษารายการการประมวลผลข้อมูลส่วนบุคคล
4) แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่ผู้ควบคุมข้อมูลส่วนบุคคลทันทีเมื่อตรวจพบ

5.3 กำหนดให้ ประธานเจ้าหน้าที่ฝ่ายการเงิน และผู้จัดการแผนกทรัพยากรบุคคล ดำรงตำแหน่ง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) เพื่อให้มีหน้าที่ให้คำแนะนำ และตรวจสอบการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลให้ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

5.4 แผนกทรัพยากรบุคคลเป็นส่วนงานที่สำคัญ และทำหน้าที่เก็บรวบรวม ประมวลผล เปิดเผยและจัดเก็บข้อมูลส่วนบุคคลของผู้สมัครงาน และพนักงาน จึงกำหนดให้บุคลากรแผนกทรัพยากรบุคคลมีความเข้าใจถึงข้อกาหนดของ PDPA เพื่อให้สามารถนำไปใช้กับการปฏิบัติงานของตนได้อย่างเหมาะสม

5.5 กำหนดให้ต้องตรวจสอบให้แน่ใจว่าพนักงานเก็บรวบรวมและประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงประโยชน์โดยชอบด้วยกฎหมาย โดยมีมาตรการรักษาความปลอดภัยที่เพียงพอ รวมทั้งมีการจัดอบรมเพื่อเป็นการย้ำหน้าที่ความรับผิดชอบในเรื่อง PDPA แก่พนักงานในบริษัทฯ และเพื่อสนับสนุนให้มีการเพิ่มพูนการตระหนักรู้และปฏิบัติตามข้อกำหนด PDPA อย่างยั่งยืน

5.6 ข้อมูลสองประเภทที่เกี่ยวข้องกับ PDPA ได้แก่ (1) ข้อมูลส่วนบุคคลและ (2) ข้อมูลส่วนบุคคลที่ละเอียดอ่อนและเนื่องจาก PDPA ใช้มาตรการความปลอดภัยที่เข้มงวดยิ่งขึ้นสำหรับข้อมูลส่วนบุคคลที่

ละเอียดอ่อน องค์กรจึงจำเป็นต้องจำแนกข้อมูล (Data Classification) ที่ตนรวบรวมในปัจจุบัน ว่าเป็นข้อมูลส่วนบุคคลหรือข้อมูลส่วนบุคคลที่ละเอียดอ่อน เพื่อจะได้ใช้วิธีบริหารจัดการข้อมูลอย่างเหมาะสม

5. ผังกระบวนการทำงาน

ประกอบด้วยกระบวนการทำงาน ดังรายละเอียดต่อไปนี้

5.1 กระบวนการขึ้นทะเบียนลูกค้าและ การจัดการฐานข้อมูลลูกค้า

5.2 กระบวนการขึ้นทะเบียนผู้ขายและคู่ค้า และ การจัดการฐานข้อมูล

5.3 กระบวนการสรรหาพนักงาน

5.4 การจ้างพนักงาน การจ่ายผลตอบแทน และการประเมินผลพนักงาน

5.5 กระบวนการลาออกของพนักงาน

ดูรายละเอียดใน **"เอกสารแนบ"** ระเบียบปฏิบัติงาน

6. ระเบียบปฏิบัติงาน

6.1 หน้าที่และความรับผิดชอบ

6.1.1 คณะกรรมการ

1) กำหนดให้มีนโยบายคุ้มครองข้อมูลส่วนบุคคล
2) กำกับดูแลให้มีการนำนโยบายไปปฏิบัติอย่างเป็นรูปธรรม

6.1.2 ผู้บริหาร

1) จัดให้มีระเบียบปฏิบัติงานและมาตรการในการจัดเก็บข้อมูลส่วนบุคคลให้เหมาะสมกับบริบทของแต่ละบริษัทโดยให้สอดคล้องกับนโยบายและแนวปฏิบัติ กฎหมายของแต่ละประเทศที่บริษัทประกอบธุรกิจ และมาตรฐานสากล
2) จัดให้มีโครงสร้างผู้รับผิดชอบเพื่อดูแลการดำเนินงานให้เป็นไปตามระเบียบปฏิบัติ
3) จัดให้มีระบบการคัดเลือกบุคคลหรือนิติบุคคลที่มีระบบการคุ้มครองข้อมูลที่ได้มาตรฐานและสอดคล้องตามกฎหมาย ในกรณีที่บริษัทว่าจ้างบุคคลหรือนิติบุคคลอื่นให้ดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลแทน

4) กำกับดูแลให้มีการปฏิบัติตามนโยบาย แนวปฏิบัติ และระเบียบปฏิบัติ ตลอดจนพัฒนาปรับปรุงวิธีการปฏิบัติให้มีประสิทธิภาพ รวมทั้งให้มีการรายงานผลอย่างสม่ำเสมอ

6.1.3 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

1) ควบคุม และตรวจสอบการดำเนินการของบริษัทให้ถูกต้องตามที่กฎหมายกำหนด รวมถึงการจัดกิจกรรมสร้างความตระหนักรู้ ตลอดจนการฝึกอบรมที่เกี่ยวข้องกับการดำเนินงานด้านข้อมูลส่วนบุคคล
2) ให้คำปรึกษาและแนะนำคณะกรรมการ ผู้บริหาร และพนักงาน ในการปฏิบัติตามกฎหมายให้ถูกต้อง
3) เป็นศูนย์กลางในการติดต่อเรื่องข้อมูลส่วนบุคคล การปกป้องสิทธิของเจ้าของข้อมูล รวมถึงการประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
4) รักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่

6.1.4 พนักงาน

1) ใช้ข้อมูลส่วนบุคคลอย่างระมัดระวัง ปฏิบัติตามกฎหมาย กฎระเบียบ ข้อบังคับของบริษัทอย่างเคร่งครัด
2) แจ้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทันที เมื่อพบการรั่วไหลหรือการละเมิดของข้อมูลส่วนบุคคล
3) หากพบเห็นการกระทำที่อาจเข้าข่ายเป็นการฝ่าฝืนนโยบายฉบับนี้ ให้แจ้งผ่านช่องทางการแจ้งเบาะแสและข้อร้องเรียนของบริษัท

6.2 แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

6.2.1 การเก็บรวบรวมข้อมูลส่วนบุคคล

1) จัดเก็บข้อมูลส่วนบุคคลอย่างจำกัดเท่าที่จำเป็นแก่การใช้งานตามวัตถุประสงค์ที่ได้แจ้งแก่ เจ้าของข้อมูลส่วนบุคคล

2) ไม่จัดเก็บข้อมูลส่วนบุคคลที่เป็นข้อมูลที่อ่อนไหวหรือข้อมูลที่ก่อให้เกิดการเลือกปฏิบัติโดยไม่เป็นธรรม หรือความไม่เท่าเทียมกัน ซึ่งอาจส่งผลกระทบต่อเจ้าของข้อมูล เว้นแต่เป็นการจัดเก็บตามกฎหมาย

6.2.2 การเก็บรักษาข้อมูลส่วนบุคคล

1) ต้องมีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูลส่วนบุคคล เพื่อป้องกันการทำลาย การดัดแปลง แก้ไขและการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และเพื่อป้องกันไม่ให้เกิดการรั่วไหลข้อมูลส่วนบุคคล

2) การจัดเก็บข้อมูลส่วนบุคคลโดยบุคคลภายใน บุคคลภายนอก หรือบริษัทภายนอกต้องมีระบบการคุ้มครอง ข้อมูลตามมาตรฐานสากล มีข้อตกลงการเก็บรักษาข้อมูลส่วนบุคคลตามวัตถุประสงค์เท่าที่จำเป็นแก่การใช้งาน

6.2.3 การส่งหรือโอนข้อมูลส่วนบุคคล

1) การส่งหรือโอนข้อมูลส่วนบุคคลต้องได้รับการร้องขอหรือให้ความยินยอมจากเจ้าของข้อมูลเป็นลายลักษณ์อักษร

2) การโอนข้อมูลส่วนบุคคลระหว่างประเทศสามารถทำได้ในกรณีดังต่อไปนี้

2.1 เจ้าของข้อมูลส่วนบุคคลรับทราบถึงมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลของประเทศปลายทางที่อาจมีไม่เพียงพอ พร้อมทั้งได้ให้การยินยอม

2.2 การโอนข้อมูลส่วนบุคคลเป็นการจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญา หรือเป็นการดำเนินการตามคำร้องขอของเจ้าของข้อมูลส่วนบุคคล

2.3 การโอนข้อมูลส่วนบุคคลได้ทำเพื่อป้องกันหรือระงับอันตรายต่อชีวิต หรือสุขภาพของเจ้าของข้อมูลส่วนบุคคล ในกรณีที่เจ้าของข้อมูลส่วนบุคคลไม่สามารถให้การยินยอมได้

6.2.4 สิทธิเจ้าของข้อมูลส่วนบุคคล

1) สิทธิขอเข้าถึงและขอรับสำเนาข้อมูลส่วนบุคคลที่เกี่ยวกับตน หรือขอให้เปิดเผยถึงการได้มาซึ่งข้อมูลส่วนบุคคลดังกล่าวที่ตนไม่ได้ให้ความยินยอม

2) สิทธิขอให้ดำเนินการลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล

3) สิทธิในการขอให้ระงับการใช้ข้อมูลส่วนบุคคล

4) สิทธิในการเพิกถอนความยินยอมในการประมวลผลข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไว้ ทั้งนี้ การเพิกถอนความยินยอมย่อมไม่ส่งผลกระทบต่อการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้ให้ความยินยอมไว้แล้ว

5) สิทธิในการแก้ไขข้อมูลส่วนบุคคล

6) สิทธิในการขอให้โอนย้ายข้อมูลส่วนบุคคลไปยังผู้ควบคุมข้อมูลส่วนบุคคลอื่น เว้นแต่โดยสภาพไม่สามารถทำได้

7) สิทธิขอคัดค้านการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลของท่านในเวลาใดก็ได้

8) สิทธิในการร้องเรียนกรณีฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย

9) การใช้สิทธิอาจถูกจำกัดภายใต้กฎหมายที่เกี่ยวข้อง บริษัทอาจปฏิเสธการใช้สิทธิหรือไม่อาจดำเนินการตามคำขอของเจ้าของข้อมูลในบางกรณี เช่น เพื่อประโยชน์สาธารณะ ต้องปฏิบัติตามกฎหมายหรือคำสั่งของศาล ทั้งนี้บริษัทจะแจ้งให้เจ้าของข้อมูลทราบถึงเหตุผลของการปฏิเสธคำขอด้วย

6.2.5 การใช้หรือเปิดเผยข้อมูลส่วนบุคคล

1) ไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลนอกเหนือไปจากวัตถุประสงค์ และไม่เปิดเผยต่อบุคคลภายนอก หรือบริษัทภายนอก ยกเว้นเป็นไปตามที่กฎหมายกำหนด

2) ห้ามบุคลากร บุคคลภายนอก หรือบริษัทภายนอกนำข้อมูลส่วนบุคคลไปใช้ในทางที่ผิดกฎหมายและต้องปฏิบัติตามนโยบาย และกฎหมายคุ้มครองข้อมูลส่วนบุคคล

6.2.6 การทำลายข้อมูลส่วนบุคคล

1) ในกรณีข้อมูลส่วนบุคคลที่จัดเก็บนั้นไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ หรือเมื่อเจ้าของข้อมูลส่วนบุคคลคัดค้านหรือถอดถอนความยินยอม ในการประมวลข้อมูลส่วนบุคคล ให้ทำลายและลบข้อมูลออกจากระบบการจัดเก็บโดยวิธีการที่ปลอดภัยและไม่ให้ข้อมูลรั่วไหล

2) ทำลายและลบข้อมูลส่วนบุคคลออกจากระบบการจัดเก็บเมื่อพ้นระยะเวลาการใช้งานตามวัตถุประสงค์ เว้นแต่ในกรณีที่ต้องเก็บรักษาข้อมูลไว้ตามที่กฎหมายกำหนด

3) หากข้อมูลที่ต้องการทำลายจัดเก็บในรูปเอกสาร ให้ทำลายโดยวิธีย่อยทำลาย หากข้อมูลจัดเก็บในรูปไฟล์ข้อมูล ให้ดำเนินการทำลายเช่นเดียวกับการทำลายข้อมูลสำรองของระบบสารสนเทศ โดยทำเรื่องทำลายโดยใช้ FM-IT-17 และเป็นไปตามระเบียบปฏิบัติงาน SP-IT-03 : การบริหารจัดการข้อมูลฯ ทั้งนี้กำหนดให้ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) เข้าร่วมสังเกตการณ์การทำลายข้อมูลดังกล่าว

6.2.7 ระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล

บริษัทจะเก็บรักษาข้อมูลส่วนบุคคลตามระยะเวลาที่กฎหมายกำหนด หรือเท่าที่จำเป็นเพื่อบรรลุวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลดังกล่าว และจะดำเนินการจัดเก็บ ลบ หรือทำลายข้อมูลส่วนบุคคลให้เป็นไปตามมาตราฐานที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด

กรณีที่ไม่สามารถระบุระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลได้ชัดเจน บริษัทจะเก็บรักษาข้อมูลไว้ตามระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม เช่น อายุความตามกฎหมายทั่วไปสูงสุด 10 ปี

6.3 แนวปฏิบัติการคุ้มครองความเป็นส่วนตัว

เพื่อเป็นการปฏิบัติตามกฎหมายที่กำหนดเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล เว็บไซต์ของบริษัท เอส.เอ.เอฟ. สเปเชียล สตีล จำกัด (มหาชน) ต้องมีประกาศความเป็นส่วนตัวที่แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลผ่านการใช้คุกกี้ ตั้งอยู่ในตำแหน่งที่สามารถเข้าถึงง่ายบนหน้าหลักของเว็บไซต์ เขียนเป็นภาษาที่กระชับ โปร่งใส และเข้าใจง่าย โดยมีการแจ้งถึงรายละเอียดการรวบรวมข้อมูลส่วนบุคคลของผู้เข้าใช้อย่างน้อยตามหัวข้อดังต่อไปนี้

1) อธิบายถึงวัตถุประสงค์และวิธีการเก็บข้อมูลส่วนบุคคลของผู้ใช้งาน
2) ระบุถึงข้อมูลส่วนบุคคลที่เก็บรวบรวมทั้งหมดของผู้ใช้งาน (ตัวอย่าง เช่น ชื่อ ที่อยู่ หมายเลขโทรศัพท์ อีเมล หมายเลขไอพี เป็นต้น)
3) ระบุสิทธิทั้งหมดของผู้ใช้งานในฐานะเจ้าของข้อมูลส่วนบุคคล
4) เปิดสิทธิให้ผู้ใช้งานให้การยินยอม (opt-in) และปฏิเสธการยินยอม (opt-out) จากการจัดเก็บข้อมูลส่วนบุคคล

5) ระบุถึงมาตรการที่ดำเนินการทั้งหมดเพื่อปกป้องข้อมูลส่วนบุคคลของผู้ใช้งาน

6) ระบุช่องทางการติดต่อผู้ควบคุมข้อมูลส่วนบุคคล หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (ถ้ามี) เพื่อให้ผู้ใช้งานสามารถสอบถามเพิ่มเติม หรือใช้สิทธิในฐานะเจ้าของข้อมูลส่วนบุคคล

7) มีการแจ้งถึงลิงค์ภายในเว็บไซต์ที่เชื่อมโยงไปยังเว็บไซต์ของบุคคลภายนอก หรือบริษัทภายนอก ซึ่งอาจมีการเก็บข้อมูลส่วนบุคคลเพิ่มเติม ทั้งนี้ เจ้าของเว็บไซต์ดังกล่าวต้องมีประกาศความเป็นส่วนตัวเพื่อปกป้องข้อมูลส่วนบุคคลของผู้ใช้งานด้วย

6.4 กฎหมาย ข้อกำหนดและมาตรฐานสากลที่เกี่ยวข้อง

1) กฎหมายคุ้มครองข้อมูลส่วนบุคคลของแต่ละประเทศที่บริษัท เอส.เอ.เอฟ. สเปเชียล สตีล จำกัด (มหาชน) ประกอบธุรกิจ

2) การคุ้มครองข้อมูลส่วนบุคคลตามแนวทางขององค์กรเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)

3) แนวทางการควบคุมข้อมูลส่วนบุคคลที่จัดเก็บด้วยคอมพิวเตอร์ (Guidelines for the Regulation of Computerized Personal Data Files ของ Office of the United Nations High Commissioner for Human Rights: OHCHR)

6.5 บทลงโทษ

ในกรณีที่ผู้บริหารและพนักงานกระทำการใด ๆ ที่เป็นการฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและวิธีปฏิบัติงานการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าทางตรงหรือทางอ้อม ผู้บริหารและพนักงานจะถูกพิจารณาโทษทางวินัยตามระเบียบข้อบังคับการทำงานของแต่ละบริษัท

7. <u>เอกสารอ้างอิง</u>

- PC-MG-13 นโยบายคุ้มครองข้อมูลส่วนบุคคล
- นโยบายความเป็นส่วนตัว (Privacy Policy)

8. <u>บันทึกคุณภาพ</u>

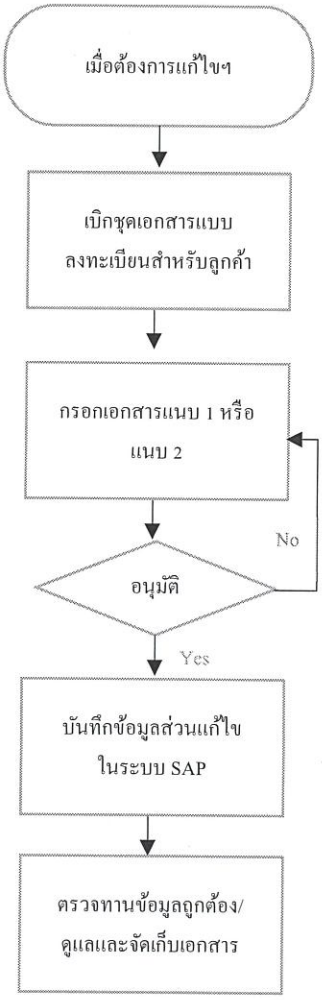
ลำดับ	หมายเลขเอกสาร	ชื่อเอกสาร	ระยะเวลาจัดเก็บ	การจัดเรียง	สถานที่เก็บ	ผู้รับผิดชอบ
1	FM-HR-29	บันทึกข้อความ (MEMO)	เก็บตามเอกสารหลักที่ใช้ memo เป็นเอกสารประกอบ	ตามวันที่	DPO	DPO
2	FM-IT-17	เอกสารขอดำเนินการกับข้อมูลสำรองระบบเทคโนโลยีสารสนเทศ	1 ปี	ตามวันที่	IT	IT
3	-	เอกสารแสดงความยินยอม (Consent Form)	ตาม VRF/CRF จนกว่าจะมีการขอเปลี่ยนแปลง	VRF/CRF	DPO	DPO

9. <u>เอกสารแนบท้าย</u>

เอกสารแนบผังกระบวนการทำงานและสรุปความเสี่ยงด้าน PDPA

***เอกสารแนบท้าย* 6.1) กระบวนการขึ้นทะเบียนลูกค้าใหม่ และ การจัดการฐานข้อมูลลูกค้า**

ผังกระบวนการ	ขั้นตอนการปฏิบัติงาน	ผู้รับผิดชอบ	เอกสาร
1. การจัดการฐานข้อมูลลูกค้าใหม่			
เมื่อต้องการเพิ่มฐานข้อมูลลูกค้ารายใหม่			
จัดทำเอกสารแบบลงทะเบียนสำหรับลูกค้าฯ	1. จัดทำเอกสาร "แบบลงทะเบียนสำหรับลูกค้า (Customer Registration Form)"	แผนกประสานงานขาย (SC)	FM-SA-13 : แบบลงทะเบียนสำหรับลูกค้า (CRF)
อนุมัติ (No)	2. เสนอให้ผู้มีอำนาจลงนามอนุมัติการขาย	ตามอำนาจอนุมัติ	
อนุมัติ (Yes)			
พิจารณาอนุมัติเงื่อนไขชำระเงินและวงเงินสินเชื่อ (ถ้ามี)	3. พิจารณาอนุมัติเงื่อนไขชำระเงินและวงเงินสินเชื่อ (ถ้ามี)	ตามอำนาจอนุมัติ	
บันทึกรายละเอียดลูกค้าในระบบ SAP B1	4. บันทึกข้อมูลลูกค้าในระบบ SAP B1	ฝ่ายบัญชีและการเงิน	
ตรวจทานข้อมูลที่บันทึกในระบบ SAP B1 และเอกสาร	5. ตรวจทานข้อมูลที่บันทึกในระบบ SAP B1 และเอกสาร	ฝ่ายบัญชีและการเงิน	
ดูแลและจัดเก็บเอกสาร	6. ดูแลและจัดเก็บเอกสาร	ประธานเจ้าหน้าที่ฝ่ายการเงิน (CFO)	

ผังกระบวนการ	ขั้นตอนการปฏิบัติงาน	ผู้รับผิดชอบ	เอกสาร
2. การขอแก้ไขเปลี่ยนแปลงข้อมูลการขึ้นทะเบียน **(รายละเอียดผู้ติดต่อของลูกค้าข้อมูลนิติบุคคล หรือเครดิตสินเชื่อ)**  	1. เบิกชุดเอกสาร "แบบลงทะเบียนสำหรับลูกค้า (Customer Registration Form)" (ถ้าจำเป็นในการดูข้อมูล)	แผนกประสานงานขาย (SC)	FM-SA-13 : แบบลงทะเบียนสำหรับลูกค้า (CRF)
	2. กรอกเอกสารแนบ 1 หรือ 2 (อ้างอิง FM-SA-13)	แผนกประสานงานขาย (SC)	เอกสารแนบ 1 หรือ 2 (อ้างอิง FM-SA-13)
	3. เสนอให้ผู้มีอำนาจลงนามอนุมัติ	ตามอำนาจอนุมัติ	
	4. บันทึกข้อมูลส่วนแก้ไขในระบบ SAP B1	ฝ่ายบัญชีและการเงิน	
	5. ตรวจทานข้อมูล เพื่อตรวจสอบความถูกต้องของข้อมูลที่ได้รับการแก้ไข/ ดูแลและจัดเก็บเอกสาร	ประธานเจ้าหน้าที่ฝ่ายการเงิน (CFO)	

สรุปความเสี่ยงด้าน PDPA สำหรับกระบวนการขึ้นทะเบียนลูกค้าใหม่ และ การจัดการฐานข้อมูลลูกค้า

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
1.	กระบวนการและบุคลากร	**เตรียมแบบลงทะเบียนสำหรับลูกค้า (CRF)** **ประเด็น:** การเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าที่เกินความจำเป็น **ความเสี่ยงด้าน PDPA:** การรวบรวมข้อมูลส่วนบุคคลที่มากเกินไป/ไม่จำเป็นโดยไม่มีมูลเหตุทางกฎหมายในการรวบรวมข้อมูลดังกล่าว **มาตรการแก้ไข:** 1) ดำเนินการประเมินภายในเพื่อระบุประเภทข้อมูลส่วนบุคคลที่ปัจจุบันต้องมีการรวบรวมในขั้นตอนการขึ้นทะเบียนฯ โดยพิจารณาความสมเหตุสมผลในการใช้ข้อมูลดังกล่าว ซึ่งการประเมินนี้ควรดำเนินการร่วมกับการจำแนกประเภทข้อมูล (Data Classification) 2) ปรับปรุงแบบลงทะเบียนสำหรับลูกค้า (CRF) เพื่อตัดลดการขอเอกสารข้อมูลส่วนบุคคลของลูกค้าที่ไม่จำเป็นสำหรับวัตถุประสงค์ในการขึ้นทะเบียนลูกค้าใหม่ 3) กรณีที่มีความจำเป็นต้องเก็บข้อมูล ให้พิจารณาว่าจะต้องมีการขอและได้รับคำยินยอม ก่อนรวบรวมข้อมูลส่วนบุคคล/ข้อมูลที่มีความละเอียดอ่อนจากลูกค้าหรือไม่ 4) ตรวจสอบให้มั่นใจว่ามีการระบุถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลอย่างชัดเจนในนโยบายความเป็นส่วนตัว (Privacy Policy) ของบริษัท 5) ตรวจสอบให้มั่นใจว่าพนักงานทุกคนได้รับการฝึกอบรมอย่างเพียงพอเพื่อสามารถปฏิบัติงานภายใต้ข้อกำหนด PDPA ได้ **เอกสารที่จำเป็น:** 1) นโยบายความเป็นส่วนตัว (Privacy Policy)	SA / SC	1.1

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
		2) เอกสารแสดงความยินยอม (Consent Form) 3) FM-SA-13: แบบลงทะเบียนสำหรับลูกค้า (CRF) 4) SP-SA-02: การขึ้นทะเบียนลูกค้า การพิจารณาสินเชื่อและการอนุมัติขายเกินวงเงินสินเชื่อ		
2.	กระบวนการ	**กรอกข้อมูลในแบบลงทะเบียนสำหรับลูกค้า (CRF) พร้อมแนบเอกสารประกอบ (หากมี)** **<u>ประเด็น:</u>** ลูกค้าให้ข้อมูลส่วนบุคคลตามที่บริษัทร้องขอ โดยไม่ทราบถึงวัตถุประสงค์ในการเก็บรวบรวมข้อมูล **<u>ความเสี่ยงด้าน PDPA:</u>** PDPA กำหนดให้เจ้าของข้อมูลต้องได้รับการแจ้งถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล ตลอดจนสิทธิในฐานเจ้าของข้อมูล **<u>มาตรการแก้ไข:</u>** 1) ตรวจสอบให้มั่นใจว่าลูกค้าสามารถเข้าถึงนโยบายความเป็นส่วนตัว (Privacy Policy) ของบริษัทได้โดยง่าย 2) กำหนดขั้นตอนการดำเนินงานโดยมีมาตรการควบคุมที่เหมาะสมเพื่อสนับสนุนและจัดทำบันทึกในกรณีที่ลูกค้าขอเข้าถึงข้อมูลส่วนบุคคลของตนเอง เช่น การกำหนดช่องทางการสื่อสารที่ลูกค้าสามารถร้องขอการเข้าถึงสิทธิ์ **<u>เอกสารที่จำเป็น:</u>** 1) นโยบายความเป็นส่วนตัว (Privacy Policy) 2) FM-SA-13: แบบลงทะเบียนสำหรับลูกค้า (CRF) 3) SP-SA-02: การขึ้นทะเบียนลูกค้า การพิจารณาสินเชื่อและการอนุมัติขายเกินวงเงินสินเชื่อ	SC	1.1

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
3.	กระบวนการ	**ตรวจสอบความครบถ้วนของข้อมูลในแบบลงทะเบียนสำหรับลูกค้า (CRF) และเอกสารประกอบ (หากมี)** **<u>ประเด็น:</u>** การเข้าถึงฐานข้อมูลของลูกค้า โดยไม่ได้รับอนุญาตในขั้นตอนการประมวลผลข้อมูล/เอกสาร **<u>ความเสี่ยงด้าน PDPA:</u>** การกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพออาจทำให้ข้อมูลสูญหาย รั่วไหล และมีการใช้และ/หรือประมวลผลข้อมูลส่วนบุคคลของลูกค้าอย่างไม่เหมาะสมได้ **<u>มาตรการแก้ไข:</u>** 1) ตรวจสอบให้มั่นใจว่าฐานข้อมูลของลูกค้าได้รับการดูแลรักษาอย่างเต็มที่ด้วยมาตรการรักษาความปลอดภัยที่เพียงพอ เช่น • จำกัดสิทธิ์ผู้ใช้ข้อมูลเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น • ตรวจสอบให้มั่นใจว่ามีเอกสารของลูกค้าถูกจัดเก็บในพื้นที่ที่กำหนด และจัดเก็บไว้ในตู้เก็บของหรือห้องเก็บของ ที่มีมาตรการรักษาความปลอดภัยที่เหมาะสม เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต รวมทั้งกำหนดผู้ดูแลควบคุมและรับผิดชอบ 2) ตรวจสอบให้มั่นใจว่ามีการบันทึกการแจ้งเตือนและเฝ้าติดตามดูกิจกรรมที่ต้องสงสัยในระบบ รวมถึงการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต 3) ตรวจสอบให้มั่นใจว่าได้มีการปฏิบัติงานตรวจสอบ โดยผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศเกี่ยวกับการเข้าถึงระบบและมาตรการรักษาความปลอดภัยของทุกระบบที่ใช้งาน 4) ตรวจสอบสิทธิ์การเข้าถึงของผู้ใช้อย่างสม่ำเสมอ โดยตรวจสอบอ้างอิงจากรายชื่อและตำแหน่งของพนักงานในปัจจุบัน	AC/ IT	1.4

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
		<u>เอกสารที่จำเป็น:</u> 1) FM-SA-13: แบบลงทะเบียนสำหรับลูกค้า (CRF) 2) SP-SA-02: การขึ้นทะเบียนลูกค้า การพิจารณาสินเชื่อและการอนุมัติขายเกินวงเงินสินเชื่อ 3) PC-IT-01: นโยบายการรักษาความปลอดภัยสารสนเทศ 4) FM-DC-01: ใบขอดำเนินการเอกสาร/Document Action Request (DAR)		
4	กระบวนการ	**กำหนดวงเงินสินเชื่อ** **<u>ประเด็น:</u>** ลูกค้าไม่ทราบถึงมีการเก็บรวบรวมข้อมูลส่วนบุคคลของตนเองจากแหล่งอื่น **<u>ความเสี่ยงด้าน PDPA:</u>** PDPA กำหนดให้เจ้าของข้อมูลต้องได้รับการแจ้งถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งข้อมูลอื่นๆ ภายใต้ฐานทางกฎหมาย **<u>มาตรการแก้ไข:</u>** กำหนดให้มีการระบุในนโยบายความเป็นส่วนตัว (Privacy Policy) ของบริษัทอย่างชัดเจนเกี่ยวกับแหล่งข้อมูลที่บริษัทจะใช้ในการเก็บรวบรวมข้อมูลส่วนบุคคลของลูกค้าเพิ่มเติม เพื่อทำการประเมินเครดิตของลูกค้า และกิจกรรมที่เกี่ยวข้องอื่น ๆ **เอกสารที่จำเป็น:** 1) นโยบายความเป็นส่วนตัว (Privacy Policy)	AC	1.3

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
5.	กระบวนการ	**ดำเนินการบันทึกรายละเอียดลูกค้าในระบบ SAP** **<u>ประเด็น:</u>** ความไม่ครบถ้วนหรือไม่ถูกต้องของข้อมูล ที่บันทึกในระบบ **<u>ความเสี่ยง:</u>** ความไม่ถูกต้องและสมบูรณ์ของข้อมูลอาจนำไปสู่บทลงโทษตามกฎหมาย **<u>มาตรการแก้ไข:</u>** กำหนดมาตรการรักษาความปลอดภัย (เช่น ขั้นตอนการตรวจสอบและอนุมัติการบันทึกข้อมูลเข้าระบบ) เพื่อให้มั่นใจว่าข้อมูลที่บันทึกเข้าในระบบครบถ้วนและถูกต้อง **<u>เอกสารที่จำเป็น:</u>** 1) SP-SA-02 : การขึ้นทะเบียนลูกค้า การพิจารณาสินเชื่อและการอนุมัติขายเกินวงเงินสินเชื่อ 2) FM-SA-13 : แบบลงทะเบียนสำหรับลูกค้า (CRF)	AC	1.4
6.	ระบบและกระบวนการ	**ดำเนินการบันทึกรายละเอียดลูกค้าในระบบ SAP** **<u>ประเด็น:</u>** การแก้ไขข้อมูลของลูกค้าในระบบโดยไม่ได้รับอนุญาต **<u>ความเสี่ยงด้าน PDPA:</u>** มาตรการรักษาความปลอดภัยของข้อมูลที่ไม่เพียงพออาจนำไปสู่ความไม่สมบูรณ์ของข้อมูล	AC	2.4

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
		มาตรการแก้ไข: 1) จัดให้มีการควบคุมด้านความปลอดภัยโดยการกำหนดสิทธิ์ตามระดับของพนักงาน เช่น สิทธิในการสร้างบัญชีลูกค้าและสิทธิในการดูข้อมูล 2) หากมีการเปลี่ยนแปลงข้อมูลในระบบ ควรมีการตรวจสอบให้แน่ใจด้วยว่ามีมาตรการควบคุมเพื่อป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต เช่น กำหนดให้มีการขออนุมัติหากพนักงานต้องการแก้ไขเปลี่ยนแปลงข้อมูล รวมถึงให้มีการตรวจสอบหลักฐานก่อนการอนุมัติแก้ไขข้อมูล (เช่น ใบคำขอเปลี่ยนแปลงข้อมูลของลูกค้า เป็นต้น) 3) กำหนดให้มีกระบวนการติดตาม ซึ่งรวมถึงแต่ไม่จำกัดเพียง: • ตรวจสอบบันทึกการเข้าถึงข้อมูลในระบบอย่างสม่ำเสมอ • ตรวจสอบความขัดแย้งของสิทธิเข้าถึงของผู้ใช้งาน เช่น ความขัดแย้งระหว่างตำแหน่งของพนักงานและส่วนงานที่สามารถเข้าถึงได้ • ดำเนินการปฏิบัติงานตรวจสอบ เพื่อให้มั่นใจว่าได้มีการยกเลิกสิทธิการเข้าถึงของพนักงานที่ลาออกไปแล้วทันทีหรือไม่ และมีการให้สิทธิ์เข้าถึงแก่พนักงานที่หมุนเวียนเปลี่ยนงาน/ได้รับการเลื่อนตำแหน่งอย่างถูกต้องตามตำแหน่งงานใหม่ที่ได้รับหรือไม่ 4) ตรวจสอบความเหมาะสมและความถูกต้องของโครงสร้างอนุมัติในระบบเป็นประจำทุกปี โดยเทียบกับโครงสร้างการอนุมัติที่กำหนดไว้ในนโยบายของบริษัท เพื่อเป็นมาตรการควบคุมเชิงป้องกัน 5) ตรวจสอบกระบวนการให้สิทธิ์เข้าถึงแก่พนักงาน เพื่อให้มั่นใจว่ามีมาตรการควบคุมที่เหมาะสม **เอกสารที่จำเป็น:** 1) SP-SA-02 : การขึ้นทะเบียนลูกค้า การพิจารณาสินเชื่อและการอนุมัติขายเกินวงเงินสินเชื่อ 2) FM-SA-13 : แบบลงทะเบียนสำหรับลูกค้า (CRF)		

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
7.	ระบบและกระบวนการ	จัดเก็บเอกสารทั้งหมด <u>ประเด็น:</u> บุคคลภายในและภายนอกสามารถเข้าถึงข้อมูลส่วนบุคคลของลูกค้าโดยไม่ได้รับอนุญาต <u>**ความเสี่ยงด้าน PDPA:**</u> มาตรการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพออาจทำให้ข้อมูลสูญหาย รั่วไหล และมีการใช้และ/หรือประมวลผลข้อมูลส่วนบุคคลของลูกค้าอย่างไม่เหมาะสมได้ <u>มาตรการแก้ไข:</u> ***การเข้าถึงทางกายภาพ*** 1) ควรจำกัดการเข้าถึงเอกสารข้อมูลส่วนบุคคลของลูกค้าให้เฉพาะพนักงานที่เกี่ยวข้องเท่านั้น 2) กำหนดให้มีกระบวนการในการขอเข้าถึงข้อมูลส่วนบุคคลของลูกค้า โดยต้องได้รับการอนุมัติจากผู้มีอำนาจ และต้องมีการบันทึกการเข้าถึงลงในสมุดคุมการขอเข้าถึงเอกสารลูกค้า โดยสามารถวางสมุดคุมนี้ บนตู้เก็บเอกสารได้ (หากสามารถดาเนินการได้) 3) ตรวจสอบให้มั่นใจว่าตู้หรือห้องเก็บเอกสารที่ใช้เก็บข้อมูลส่วนบุคคลและข้อมูลละเอียดอ่อนมีมาตรการรักษาความปลอดภัยที่เหมาะสม เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต 4) หมั่นตรวจสอบและสังเกตการณ์บริเวณทำงานและหน้าจอคอมพิวเตอร์ของพนักงาน เพื่อสนับสนุนให้เกิดวัฒนธรรมที่ดีภายในองค์กรในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ***การเข้าถึงระบบ*** 1) กำหนดมาตรการรักษาความปลอดภัย เช่น การเข้ารหัสข้อมูลเพื่อคุ้มครองข้อมูลที่มีความละเอียดอ่อน	AC	1.6, 2.5

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
		2) อัปเดตซอฟต์แวร์รักษาความปลอดภัยอยู่เสมอ เพื่อยกระดับมาตรการรักษาความปลอดภัยและเป็นการป้องกันภัยคุกคามทางไซเบอร์ (Cyber Attack) 3) ตรวจสอบและแก้ไขสิทธิ์เข้าถึงระบบอย่างสม่ำเสมอ โดยตรวจสอบจากรายชื่อพนักงานและตำแหน่งงานในปัจจุบัน 4) ตรวจสอบให้มั่นใจว่ามีการบันทึกกิจกรรมทั้งหมดที่เกิดขึ้นในระบบลงในข้อมูลจราจรคอมพิวเตอร์ (Log File) เพื่อเป็นแนวทางในการตรวจสอบ (Audit Trail) **<u>เอกสารที่จำเป็น:</u>** 1) SP-SA-02 : การขึ้นทะเบียนลูกค้า การพิจารณาสินเชื่อและการอนุมัติขายเกินวงเงินสินเชื่อ 2) PC-IT-01 : นโยบายการรักษาความปลอดภัยสารสนเทศ		
8.	กระบวนการ	**จัดเก็บเอกสารทั้งหมด** **<u>ประเด็น:</u>** การจัดเก็บข้อมูลส่วนบุคคลของลูกค้าในระยะเวลาเกินกว่าที่จำเป็น โดยไม่มีการทบทวนระยะเวลาการจัดเก็บ **<u>ความเสี่ยงด้าน PDPA:</u>** การเก็บรักษาข้อมูลส่วนบุคคลนานกว่าที่ข้อกำหนดในการเก็บรักษาข้อมูลตาม PDPA กำหนด สามารถนำไปสู่ 1) การสูญเสียความสมบูรณ์ของข้อมูลที่เกิดจากการประมวลผลข้อมูลส่วนบุคคลของลูกค้าที่ไม่เป็นปัจจุบัน 2) การใช้ และ/หรือการประมวลผลข้อมูลส่วนบุคคลของลูกค้าที่ไม่เหมาะสม	AC	1.6, 2.5

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
		มาตรการแก้ไข: 1) กำหนดระยะเวลาในการทบทวนข้อมูลส่วนบุคคลของลูกค้า เพื่อตรวจสอบให้มั่นใจว่าข้อมูลของลูกค้าถูกต้อง เป็นปัจจุบัน และไม่ถูกใช้ในทางที่ไม่เหมาะสม 2) ตรวจสอบให้แน่ใจว่ามีการกำหนดขั้นตอนการเก็บรักษา แก้ไข และลบข้อมูล พร้อมทั้งมาตรการควบคุมที่เหมาะสม 3) กำหนดมาตรการควบคุมที่เหมาะสมและเพียงพอในการบันทึกกิจกรรมการลบข้อมูลลูกค้าจากที่เก็บเอกสาร ฐานข้อมูล และเซิร์ฟเวอร์ที่ใช้สำรองข้อมูลของบริษัท 4) จัดทำมาตรการรักษาความปลอดภัย เพื่อป้องกันมิให้มีการแก้ไขและเปิดเผยข้อมูลส่วนบุคคลของลูกค้าโดยไม่ได้รับอนุญาต เช่น จำกัดการเข้าถึงให้เฉพาะสำหรับพนักงานที่เกี่ยวข้องเท่านั้น 5) ปฏิบัติงานตรวจสอบภายในอย่างสม่ำเสมอ เพื่อประเมินประสิทธิภาพในกระบวนการลบ/ทำลายข้อมูล 6) แจ้งให้พนักงานและผู้ที่รับผิดชอบทราบถึงนโยบายคุ้มครองข้อมูลส่วนบุคคลในส่วนของการเก็บรักษาข้อมูล และการดำเนินการเพื่อให้มั่นใจว่ามีการปฏิบัติตามตารางระยะการเก็บรักษาข้อมูล 7) ตรวจสอบให้มั่นใจว่าพนักงานทุกคนสามารถเข้าถึงนโยบายคุ้มครองข้อมูลส่วนบุคคลในส่วนของการเก็บรักษาข้อมูล ได้โดยง่าย **เอกสารที่จำเป็น:** 1) SP-SA-02 : การขึ้นทะเบียนลูกค้า การพิจารณาสินเชื่อและการอนุมัติขายเกินวงเงินสินเชื่อ 2) PC-MG-13 : นโยบายการคุ้มครองข้อมูลส่วนบุคคล 3) PC-IT-01 : นโยบายการรักษาความปลอดภัยสารสนเทศ		

เอกสารแนบท้าย 6.2) กระบวนการขึ้นทะเบียนผู้ขายและคู่ค้า และ การจัดการฐานข้อมูล

ผังกระบวนการ	ขั้นตอนการปฏิบัติงาน	ผู้รับผิดชอบ	เอกสาร
1. การขึ้นทะเบียนผู้ขายและคู่ค้า			
เมื่อต้องการเพิ่มฐานข้อมูลรายใหม่			
จัดทำ Vendor code Registration Form (VRF)	1. จัดทำเอกสาร Vendor code Registration Form (VRF) พร้อมแนบเอกสารประกอบ (ถ้ามี)	แผนกจัดหา/ /ฝ่ายบัญชีและการเงิน	FM-PU-14 FM-PU-15
อนุมัติ (No)	2. เสนอให้ผู้มีอำนาจลงนามอนุมัติการขาย	ตามอำนาจอนุมัติ	
Yes			
บันทึกรายชื่อผู้ขาย/ผู้ให้บริการรายใหม่ ในระบบ SAP B1	3. บันทึกข้อมูลลูกค้าในระบบ SAP B1	แผนกจัดหา	
ตรวจทานข้อมูลที่บันทึกในระบบ SAP B1 และเอกสาร	4. ตรวจทานข้อมูลที่บันทึกในระบบ SAP B1 และเอกสาร	ฝ่ายบัญชีและการเงิน	
ดูแลและจัดเก็บเอกสาร	5. ดูแลและจัดเก็บเอกสาร	ประธานเจ้าหน้าที่ฝ่ายการเงิน	

ผังกระบวนการ	ขั้นตอนการปฏิบัติงาน	ผู้รับผิดชอบ	เอกสาร
2. การขอแก้ไขเปลี่ยนแปลงข้อมูลการขึ้นทะเบียน			
เมื่อต้องการแก้ไขฯ			
เบิก Vendor code Registration Form (VRF)	1. เบิกชุดเอกสาร "แบบลงทะเบียนสำหรับลูกค้า (Customer Registration Form)" (ถ้าจำเป็นในการดูข้อมูล)	แผนกจัดหา	FM-PU-14 FM-PU-15
กรอกเอกสารส่วนการขอแก้ไขฯ	2. กรอกเอกสารส่วนขอแก้ไขฯ	แผนกจัดหา	
อนุมัติ (No)	3. เสนอให้ผู้มีอำนาจลงนามอนุมัติ	ตามอำนาจอนุมัติ	
(Yes) บันทึกข้อมูลส่วนแก้ไขในระบบ SAP	4. บันทึกข้อมูลส่วนแก้ไขในระบบ SAP B1	แผนกจัดหา	
ตรวจทานข้อมูลถูกต้อง	5. ตรวจทานข้อมูล เพื่อตรวจสอบความถูกต้องของข้อมูลที่ได้รับการแก้ไข	ประธานเจ้าหน้าที่ฝ่ายการเงิน (CFO)	
ดูแลและจัดเก็บเอกสาร	6. ดูแลและจัดเก็บเอกสาร	ประธานเจ้าหน้าที่ฝ่ายการเงิน	

สรุปความเสี่ยงด้าน PDPA สำหรับกระบวนการกระบวนการขึ้นทะเบียนผู้ขายและคู่ค้า และ การจัดการฐานข้อมูล

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
1.	กระบวนการและบุคลากร	**เตรียมแบบขึ้นทะเบียนผู้ขาย / ผู้ให้บริการ (Vendor Code Registration Form : VRF)** **<u>ประเด็น:</u>** การเก็บรวบรวมข้อมูลส่วนบุคคลของคู่ค้าที่เกินความจำเป็น **<u>ความเสี่ยงด้าน PDPA:</u>** การรวบรวมข้อมูลส่วนบุคคลที่มากเกินไป/ไม่จำเป็นโดยไม่มีมูลเหตุทางกฎหมายในการรวบรวมข้อมูลดังกล่าว **<u>มาตรการแก้ไข:</u>** 1) ดำเนินการประเมินภายในเพื่อระบุประเภทข้อมูลส่วนบุคคลที่ปัจจุบันต้องมีการรวบรวมในขั้นตอนการขึ้นทะเบียนฯ โดยพิจารณาความสมเหตุสมผลในการใช้ข้อมูลดังกล่าว ซึ่งการประเมินนี้ควรดำเนินการร่วมกับการจำแนกประเภทข้อมูล (Data Classification) 2) ปรับปรุงแบบขึ้นทะเบียนผู้ขาย / ผู้ให้บริการ (VRF) เพื่อตัดลดการขอเอกสารข้อมูลส่วนบุคคลของลูกค้าที่ไม่จำเป็นสำหรับวัตถุประสงค์ในการขึ้นทะเบียนฯ 3) กรณีที่มีความจำเป็นต้องเก็บข้อมูล ให้พิจารณาว่าจะต้องมีการขอและได้รับคำยินยอม ก่อนรวบรวมข้อมูลส่วนบุคคล/ข้อมูลที่มีความละเอียดอ่อนจากลูกค้าหรือไม่ 4) ตรวจสอบให้มั่นใจว่ามีการระบุถึงวัตถุประสงค์ในการเก็บรวบรวมใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลอย่างชัดเจนในนโยบายความเป็นส่วนตัว (Privacy Policy) ของบริษัท 5) ตรวจสอบให้มั่นใจว่าพนักงานทุกคนได้รับการฝึกอบรมอย่างเพียงพอเพื่อสามารถปฏิบัติงานภายใต้ข้อกำหนด PDPA ได้ **<u>เอกสารที่จำเป็น:</u>** 1) นโยบายความเป็นส่วนตัว (Privacy Policy)	PU	1.1

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
		2) เอกสารแสดงความยินยอม (Consent Form) 3) FM-PU-14 : แบบขึ้นทะเบียนผู้ขาย / ผู้ให้บริการ 4) FM-PU-15 : Vendor Code Registration Form (VRF) 5) SP-PU-04 : การคัดเลือกผู้ขาย/ผู้ให้บริการรายใหม่		
2.	กระบวนการ	**กรอกข้อมูลในแบบขึ้นทะเบียนผู้ขาย / ผู้ให้บริการ (Vendor Code Registration Form : VRF)พร้อมแนบเอกสารประกอบ (หากมี)** **<u>ประเด็น:</u>** ผู้ขายฯ ให้ข้อมูลส่วนบุคคลตามที่บริษัทร้องขอ โดยไม่ทราบถึงวัตถุประสงค์ในการเก็บรวบรวมข้อมูล **<u>ความเสี่ยงด้าน PDPA:</u>** PDPA กำหนดให้เจ้าของข้อมูลต้องได้รับการแจ้งถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล ตลอดจนสิทธิในฐานเจ้าของข้อมูล **<u>มาตรการแก้ไข:</u>** 1) ตรวจสอบให้มั่นใจว่าลูกค้าสามารถเข้าถึงนโยบายความเป็นส่วนตัว (Privacy Policy) ของบริษัทได้โดยง่าย 2) กำหนดขั้นตอนการดำเนินงานโดยมีมาตรการควบคุมที่เหมาะสมเพื่อสนับสนุนและจัดทำบันทึกในกรณีที่ลูกค้าขอเข้าถึงข้อมูลส่วนบุคคลของตนเอง เช่น การกำหนดช่องทางการสื่อสารที่ผู้ขายสามารถร้องขอการเข้าถึงสิทธิ์ **<u>เอกสารที่จำเป็น:</u>** 1) นโยบายความเป็นส่วนตัว (Privacy Policy) 2) FM-PU-14 : แบบขึ้นทะเบียนผู้ขาย / ผู้ให้บริการ 3) FM-PU-15 : Vendor Code Registration Form (VRF) 4) SP-PU-04 : การคัดเลือกผู้ขาย/ผู้ให้บริการรายใหม่	PU	1.1

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
3.	กระบวนการ	ตรวจสอบความครบถ้วนของข้อมูลในแบบขึ้นทะเบียนผู้ขาย / ผู้ให้บริการ (Vendor Code Registration Form : VRF) และเอกสารประกอบ (หากมี) **<u>ประเด็น:</u>** การเข้าถึงฐานข้อมูลของผู้ขายฯ โดยไม่ได้รับอนุญาตในขั้นตอนการประมวลผลข้อมูล/เอกสาร **<u>ความเสี่ยงด้าน PDPA:</u>** การกำหนดมาตรการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพออาจทำให้ข้อมูลสูญหาย รั่วไหล และมีการใช้และ/หรือประมวลผลข้อมูลส่วนบุคคลของผู้ขายฯอย่างไม่เหมาะสมได้ **<u>มาตรการแก้ไข:</u>** 1) ตรวจสอบให้มั่นใจว่าฐานข้อมูลของผู้ขายฯได้รับการดูแลรักษาอย่างเต็มที่ด้วยมาตรการรักษาความปลอดภัยที่เพียงพอ เช่น • จำกัดสิทธิ์ผู้ใช้ข้อมูลเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น • ตรวจสอบให้มั่นใจว่ามีเอกสารของผู้ขายฯถูกจัดเก็บในพื้นที่ที่กำหนด และจัดเก็บไว้ในตู้เก็บของหรือห้องเก็บของ ที่มีมาตรการรักษาความปลอดภัยที่เหมาะสม เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต รวมทั้งกำหนดผู้ดูแลควบคุมและรับผิดชอบ 2) ตรวจสอบให้มั่นใจว่ามีการบันทึกการแจ้งเตือนและเฝ้าติดตามดูกิจกรรมที่ต้องสงสัยในระบบ รวมถึงการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต 3) ตรวจสอบให้มั่นใจว่าได้มีการปฏิบัติงานตรวจสอบ โดยผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศเกี่ยวกับการเข้าถึงระบบและมาตรการรักษาความปลอดภัยของทุกระบบที่ใช้งาน 4) ตรวจสอบสิทธิ์การเข้าถึงของผู้ใช้อย่างสม่ำเสมอ โดยตรวจสอบอ้างอิงจากรายชื่อและตำแหน่งของพนักงานในปัจจุบัน **<u>เอกสารที่จำเป็น:</u>** 1) FM-PU-14 : แบบขึ้นทะเบียนผู้ขาย / ผู้ให้บริการ	AC/ IT	1.4

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
		2) FM-PU-15 : Vendor Code Registration Form (VRF) 3) SP-PU-04 : การคัดเลือกผู้ขาย/ผู้ให้บริการรายใหม่ 4) PC-IT-01 : นโยบายการรักษาความปลอดภัยสารสนเทศ 5) FM-DC-01 : ใบขอดำเนินการเอกสาร/Document Action Request (DAR)		
4.	กระบวนการ	**ดำเนินการบันทึกรายละเอียดผู้ขายฯในระบบ SAP** **ประเด็น:** ความไม่ครบถ้วนหรือไม่ถูกต้องของข้อมูล ที่บันทึกในระบบ **ความเสี่ยง:** ความไม่ถูกต้องและสมบูรณ์ของข้อมูลอาจนำไปสู่บทลงโทษตามกฎหมาย **มาตรการแก้ไข:** กำหนดมาตรการรักษาความปลอดภัย (เช่น ขั้นตอนการตรวจสอบและอนุมัติการบันทึกข้อมูลเข้าระบบ) เพื่อให้มั่นใจว่าข้อมูลที่บันทึกเข้าในระบบครบถ้วนและถูกต้อง **เอกสารที่จำเป็น:** 1) FM-PU-14 : แบบขึ้นทะเบียนผู้ขาย / ผู้ให้บริการ 2) FM-PU-15 : Vendor Code Registration Form (VRF) 3) SP-PU-04 : การคัดเลือกผู้ขาย/ผู้ให้บริการรายใหม่	PU	1.3
5.	ระบบและกระบวนการ	**ดำเนินการบันทึกรายละเอียดลูกค้าในระบบ SAP** **ประเด็น:** การแก้ไขข้อมูลของผู้ขายฯในระบบโดยไม่ได้รับอนุญาต	PU	2.4

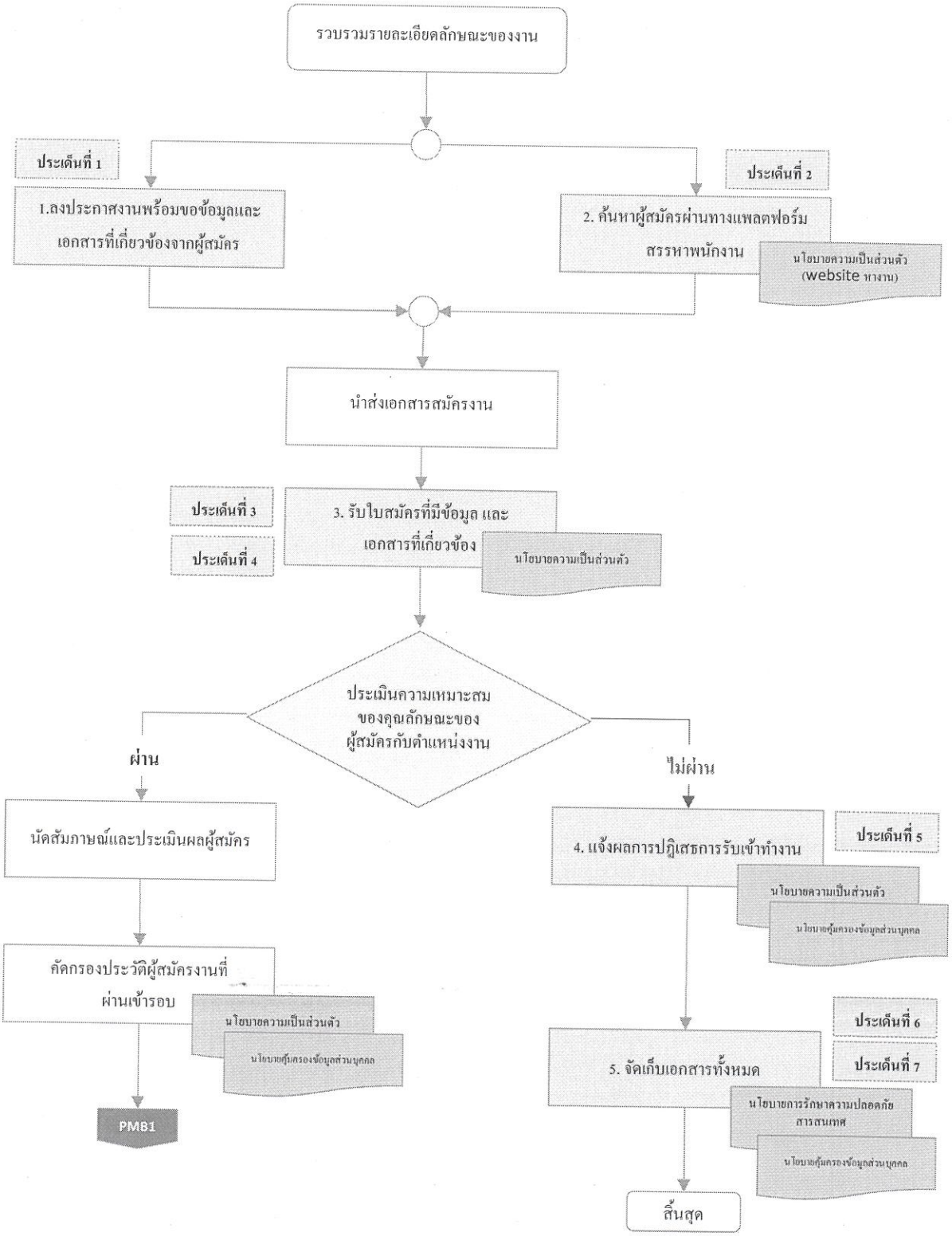
ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
		<u>ความเสี่ยงด้าน PDPA:</u> มาตรการรักษาความปลอดภัยของข้อมูลที่ไม่เพียงพออาจนำไปสู่ความไม่สมบูรณ์ของข้อมูล **<u>มาตรการแก้ไข:</u>** 1) จัดให้มีการควบคุมด้านความปลอดภัยโดยการกำหนดสิทธิ์ตามระดับของพนักงาน เช่น สิทธิในการสร้างบัญชีลูกค้าและสิทธิในการดูข้อมูล 2) หากมีการเปลี่ยนแปลงข้อมูลในระบบ ควรมีการตรวจสอบให้แน่ใจด้วยว่ามีมาตรการควบคุมเพื่อป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต เช่น กำหนดให้มีการขออนุมัติหากพนักงานต้องการแก้ไขเปลี่ยนแปลงข้อมูล รวมถึงให้มีการตรวจสอบหลักฐานก่อนการอนุมัติแก้ไขข้อมูล (เช่น ใบคำขอเปลี่ยนแปลงข้อมูลของลูกค้า เป็นต้น) 3) กำหนดให้มีกระบวนการติดตาม ซึ่งรวมถึงแต่ไม่จำกัดเพียง: • ตรวจสอบบันทึกการเข้าถึงข้อมูลในระบบอย่างสม่ำเสมอ • ตรวจสอบความขัดแย้งของสิทธิเข้าถึงของผู้ใช้งาน เช่น ความขัดแย้งระหว่างตำแหน่งของพนักงานและส่วนงานที่สามารถเข้าถึงได้ • ดำเนินการปฏิบัติงานตรวจสอบ เพื่อให้มั่นใจว่าได้มีการยกเลิกสิทธิการเข้าถึงของพนักงานที่ลาออกไปแล้วทันทีหรือไม่ และมีการให้สิทธิ์เข้าถึงแก่พนักงานที่หมุนเวียนเปลี่ยนงาน/ได้รับการเลื่อนตำแหน่งอย่างถูกต้องตามตำแหน่งงานใหม่ที่ได้รับหรือไม่ 4) ตรวจสอบความเหมาะสมและความถูกต้องของโครงสร้างอนุมัติในระบบเป็นประจำทุกปี โดยเทียบกับโครงสร้างการอนุมัติที่กำหนดไว้ในนโยบายของบริษัท เพื่อเป็นมาตรการควบคุมเชิงป้องกัน 5) ตรวจสอบกระบวนการให้สิทธิ์เข้าถึงแก่พนักงาน เพื่อให้มั่นใจว่ามีมาตรการควบคุมที่เหมาะสม **<u>เอกสารที่จำเป็น:</u>** 1) FM-PU-14 : แบบขึ้นทะเบียนผู้ขาย / ผู้ให้บริการ 2) FM-PU-15 : Vendor Code Registration Form (VRF) 3) SP-PU-04 : การคัดเลือกผู้ขาย/ผู้ให้บริการรายใหม่		

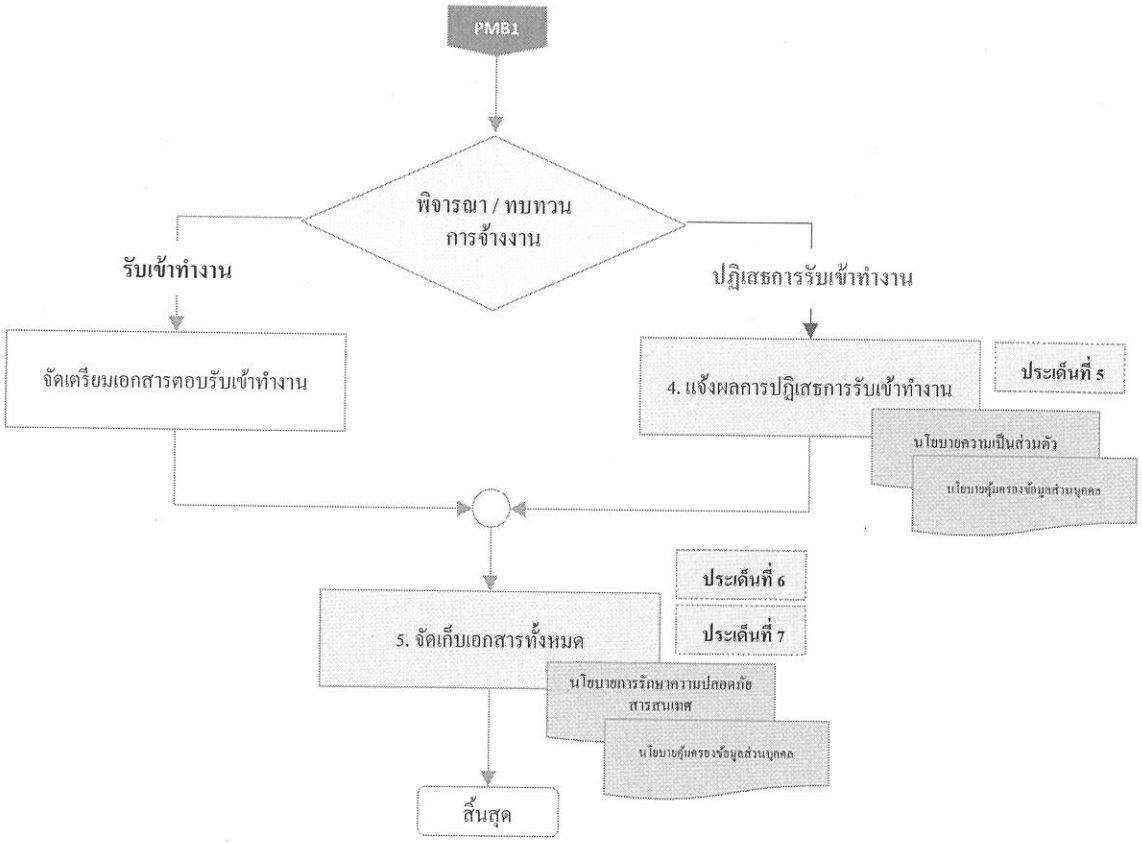
ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
6.	ระบบและกระบวนการ	จัดเก็บเอกสารทั้งหมด **<u>ประเด็น:</u>** บุคคลภายในและภายนอกสามารถเข้าถึงข้อมูลส่วนบุคคลของผู้ขายฯ โดยไม่ได้รับอนุญาต **<u>ความเสี่ยงด้าน PDPA:</u>** มาตรการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพออาจทำให้ข้อมูลสูญหาย รั่วไหล และมีการใช้และ/หรือประมวลผลข้อมูลส่วนบุคคลของลูกค้าอย่างไม่เหมาะสมได้ **<u>มาตรการแก้ไข:</u>** ***การเข้าถึงทางกายภาพ*** 1) ควรจำกัดการเข้าถึงเอกสารข้อมูลส่วนบุคคลของผู้ขายฯ ให้เฉพาะพนักงานที่เกี่ยวข้องเท่านั้น 2) กำหนดให้มีกระบวนการในการขอเข้าถึงข้อมูลส่วนบุคคลของผู้ขายฯ โดยต้องได้รับการอนุมัติจากผู้มีอำนาจ และต้องมีการบันทึกการเข้าถึงลงในสมุดคุมการขอเข้าถึงเอกสารผู้ขายฯ โดยสามารถวางสมุดคุมนี้บนตู้เก็บเอกสารได้ (หากสามารถดาเนินการได้) 3) ตรวจสอบให้มั่นใจว่าตู้หรือห้องเก็บเอกสารที่ใช้เก็บข้อมูลส่วนบุคคลและข้อมูลละเอียดอ่อนมีมาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต 4) หมั่นตรวจสอบและสังเกตการณ์บริเวณทำงานและหน้าจอคอมพิวเตอร์ของพนักงาน เพื่อสนับสนุนให้เกิดวัฒนธรรมที่ดีภายในองค์กรในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ***การเข้าถึงระบบ*** 1) กำหนดมาตรการรักษาความปลอดภัย เช่น การเข้ารหัสข้อมูลเพื่อคุ้มครองข้อมูลที่มีความละเอียดอ่อน	AC	1.5, 2.6

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
		2) อัปเดตซอฟต์แวร์รักษาความปลอดภัยอยู่เสมอ เพื่อยกระดับมาตรการรักษาความปลอดภัยและเป็นการป้องกันภัยคุกคามทางไซเบอร์ (Cyber Attack) 3) ตรวจสอบและแก้ไขสิทธิ์เข้าถึงระบบอย่างสม่ำเสมอ โดยตรวจสอบจากรายชื่อพนักงานและตำแหน่งงานในปัจจุบัน 4) ตรวจสอบให้มั่นใจว่ามีการบันทึกกิจกรรมทั้งหมดที่เกิดขึ้นในระบบลงในข้อมูลจราจรคอมพิวเตอร์ (Log File) เพื่อเป็นแนวทางในการตรวจสอบ (Audit Trail) **<u>เอกสารที่จำเป็น:</u>** 1) SP-PU-04 : การคัดเลือกผู้ขาย/ผู้ให้บริการรายใหม่ 2) PC-IT-01 : นโยบายการรักษาความปลอดภัยสารสนเทศ		
7.	กระบวนการ	**จัดเก็บเอกสารทั้งหมด** **<u>ประเด็น:</u>** การจัดเก็บข้อมูลส่วนบุคคลของผู้ขายฯในระยะเวลาเกินกว่าที่จำเป็น โดยไม่มีการทบทวนระยะเวลาการจัดเก็บ **<u>ความเสี่ยงด้าน PDPA:</u>** การเก็บรักษาข้อมูลส่วนบุคคลนานกว่าที่ข้อกำหนดในการเก็บรักษาข้อมูลตาม PDPA กำหนด สามารถนำไปสู่ 1) การสูญเสียความสมบูรณ์ของข้อมูลที่เกิดจากการประมวลผลข้อมูลส่วนบุคคลของผู้ขายฯที่ไม่เป็นปัจจุบัน 2) การใช้ และ/หรือการประมวลผลข้อมูลส่วนบุคคลของผู้ขายฯที่ไม่เหมาะสม **<u>มาตรการแก้ไข:</u>** 1) กำหนดระยะเวลาในการทบทวนข้อมูลส่วนบุคคลของผู้ขายฯ เพื่อตรวจสอบให้มั่นใจว่าข้อมูลของผู้ขายฯถูกต้อง เป็นปัจจุบัน และไม่ถูกใช้ในทางที่ไม่เหมาะสม	AC	1.5, 2.6

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผังฯ
		2) ตรวจสอบให้แน่ใจว่ามีการกำหนดขั้นตอนการเก็บรักษา แก้ไข และลบข้อมูล พร้อมทั้งมาตรการควบคุมที่เหมาะสม 3) กำหนดมาตรการควบคุมที่เหมาะสมและเพียงพอในการบันทึกกิจกรรมการลบข้อมูลผู้ขายฯจากที่เก็บเอกสาร ฐานข้อมูล และเซิร์ฟเวอร์ที่ใช้สำรองข้อมูลของบริษัท 4) จัดทำมาตรการรักษาความปลอดภัย เพื่อป้องกันมิให้มีการแก้ไขและเปิดเผยข้อมูลส่วนบุคคลของผู้ขายฯ โดยไม่ได้รับอนุญาต เช่น จำกัดการเข้าถึงให้เฉพาะสำหรับพนักงานที่เกี่ยวข้องเท่านั้น 5) ปฏิบัติงานตรวจสอบภายในอย่างสม่ำเสมอ เพื่อประเมินประสิทธิภาพในกระบวนการลบ/ทำลายข้อมูล 6) แจ้งให้พนักงานและผู้ที่รับผิดชอบทราบถึงนโยบายคุ้มครองข้อมูลส่วนบุคคลในส่วนของการเก็บรักษาข้อมูล และการดำเนินการเพื่อให้มั่นใจว่ามีการปฏิบัติตามตารางระยะการเก็บรักษาข้อมูล 7) ตรวจสอบให้มั่นใจว่าพนักงานทุกคนสามารถเข้าถึงนโยบายคุ้มครองข้อมูลส่วนบุคคลในส่วนของการเก็บรักษาข้อมูล ได้โดยง่าย <u>เอกสารที่จำเป็น:</u> 1) SP-PU-04 : การคัดเลือกผู้ขาย/ผู้ให้บริการรายใหม่ 2) PC-MG-13 : นโยบายการคุ้มครองข้อมูลส่วนบุคคล 3) PC-IT-01 : นโยบายการรักษาความปลอดภัยสารสนเทศ		

เอกสารแนบท้าย 6.3) กระบวนการสรรหาพนักงาน




PMB1
พิจารณา / ทบทวน
การจ้างงาน
รับเข้าทำงาน
ปฏิเสธการรับเข้าทำงาน
จัดเตรียมเอกสารตอบรับเข้าทำงาน
4. แจ้งผลการปฏิเสธการรับเข้าทำงาน
ประเด็นที่ 5
นโยบายความเป็นส่วนตัว
นโยบายคุ้มครองข้อมูลส่วนบุคคล
ประเด็นที่ 6
ประเด็นที่ 7
5. จัดเก็บเอกสารทั้งหมด
นโยบายการรักษาความปลอดภัย
สารสนเทศ
นโยบายคุ้มครองข้อมูลส่วนบุคคล
สิ้นสุด

สรุปความเสี่ยงด้าน PDPA สำหรับกระบวนการสรรหาพนักงาน

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
1.	กระบวนการ	**ลงประกาศงานพร้อมขอข้อมูลและเอกสารที่เกี่ยวข้องจากผู้สมัคร** **ประเด็น:** การเก็บรวบรวมและการใช้ข้อมูลส่วนบุคคล เพื่อจุดประสงค์ที่ไม่ได้ตั้งใจ **ความเสี่ยงด้าน PDPA:** การเก็บรวบรวมข้อมูลส่วนบุคคลของผู้สมัครที่มากเกินจำเป็น โดยไม่มีเหตุอันชอบภายใต้ฐานทางกฎหมายในการเก็บรวบรวมข้อมูลดังกล่าว **มาตรการแก้ไข:** 1) ดำเนินการทบทวนข้อมูลส่วนบุคคลที่ขอจากผู้สมัครในแบบฟอร์มใบสมัครงานของบริษัท ณ ปัจจุบัน โดยพิจารณาว่ามีความสมเหตุสมผลในการใช้ข้อมูลดังกล่าวเพื่อการประเมินคุณสมบัติของผู้สมัครงานหรือไม่ ซึ่งการพิจารณานี้ควรดำเนินการร่วมกับการใช้เทมเพลตการจำแนกประเภทข้อมูล (Data Classification) 2) ปรับปรุงแก้ไขแบบฟอร์มใบสมัครงาน เพื่อตัดลดการขอข้อมูลส่วนบุคคลที่ไม่จำเป็น ภายใต้ฐานทางกฎหมายในการเก็บรวบรวมข้อมูล **เอกสารที่จำเป็น:** FM-HR-17 : ใบสมัครงาน	HR	6.3.1
2.	กระบวนการ	**ค้นหาผู้สมัครผ่านทางแพลตฟอร์มสรรหาพนักงาน** **ประเด็น:** การสร้างกลุ่มคนที่มีศักยภาพสูง (Talent Pool) โดยการรวบรวมจัดเก็บข้อมูลส่วนบุคคลของคนกลุ่มนี้	HR	6.3.2

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
		ความเสี่ยงด้าน PDPA: บริษัทต้องมีฐานทางกฎหมายในการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลส่วนบุคคลโดยตรง และต้องได้รับคำยินยอมจากเจ้าของข้อมูล (หากจำเป็น) **มาตรการแก้ไข:** 1) ตรวจสอบข้อมูลของกลุ่มคนที่มีศักยภาพสูงในฐานข้อมูลของบริษัท โดยให้มีการเก็บรวบรวมข้อมูลส่วนบุคคลเฉพาะผู้ที่บริษัท มีความสนใจที่จะติดต่อเพื่อพิจารณารับเข้าทำงานเท่านั้น 2) ในการเก็บข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่จากเจ้าของข้อมูลโดยตรงสำหรับวัตถุประสงค์ในการสรรหาพนักงาน บริษัทต้องเก็บรวบรวมเฉพาะข้อมูลส่วนบุคคลอันชอบภายใต้ฐานทางกฎหมาย 3) ตรวจสอบให้แน่ชัดว่าข้อมูลส่วนบุคคลของคนกลุ่มนี้ถูกเก็บรวบรวมมาจากแหล่งที่ชอบด้วยกฎหมาย 4) จัดทำรายการตรวจสอบและสอบทานบริษัทจัดหางานและเว็บไซต์หางาน เพื่อให้มั่นใจว่ามีการบังคับใช้นโยบายความเป็นส่วนตัว (Privacy Policy) ที่เหมาะสม 5) พิจารณาขอคำแนะนำจากที่ปรึกษาทางกฎหมายเพิ่มเติม ว่าจำเป็นต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลรับทราบ และ/หรือขอคำ ยินยอม ในการเก็บรวบรวมข้อมูลส่วนบุคคลหรือไม่ **เอกสารที่จำเป็น:** 1) นโยบายความเป็นส่วนตัว (Privacy Policy) อ้างอิงตาม website หางานที่บริษัทใช้บริการ 2) FM-HR-17 : ใบสมัครงาน		
3.	กระบวนการ	**รับใบสมัครที่มีข้อมูลและเอกสารที่เกี่ยวข้อง** **ประเด็น:** ผู้สมัครงานให้ข้อมูลส่วนบุคคลตามที่บริษัทร้องขอ โดยไม่ทราบถึงสิทธิของตนเองในฐานะเจ้าของข้อมูล	HR	6.3.3

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
		<u>ความเสี่ยงด้าน PDPA:</u> PDPA กำหนดให้เจ้าของข้อมูลต้องได้รับการแจ้งถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล ตลอดจนสิทธิในฐานะเจ้าของข้อมูล **<u>มาตรการแก้ไข:</u>** 1) พิจารณาช่องทางต่าง ๆ ที่บริษัทรับเอกสารสมัครงานจากผู้สมัครงาน เช่น เว็บไซต์ของบริษัท บริษัทจัดหางาน เว็บไซต์หางานและมหกรรมจัดหางาน เป็นต้น 2) กำหนดวิธีที่เหมาะสมในการแจ้งให้ผู้สมัครงานรับทราบถึงรายละเอียดที่เกี่ยวข้อง (เช่น วัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคล ระยะเวลาเก็บรักษาข้อมูล สิทธิในฐานะเจ้าของข้อมูล และข้อมูลติดต่อของบริษัท เป็นต้น) และบันทึกการรับทราบและคำยินยอม (หากจำเป็น) ของผู้สมัครงานตามช่องทางต่าง ๆ ที่บริษัทรับเอกสารสมัครงานจากผู้สมัครงาน ได้แก่ • <u>การส่งเอกสารสมัครงานผ่านเว็บไซต์ของบริษัท:</u> พิจารณาใส่ตัวเลือก 'ฉันยอมรับข้อตกลงและเงื่อนไข' ที่แสดงในนโยบายความเป็นส่วนตัวของบริษัท (Privacy Policy) เมื่อเข้าสู่ website ของบริษัท และมีการกำหนดการยอมรับฯในส่วนสุดท้ายของแบบฟอร์มสมัครงาน เพื่อบันทึกการยินยอมของผู้สมัครงานก่อนนำส่งเอกสารให้บริษัท • <u>การส่งเอกสารสมัครงานผ่านเว็บไซต์หางานหรือบริษัทจัดหางาน:</u> ตรวจสอบว่าเว็บไซต์หางานและบริษัทจัดหางานเหล่านี้ปฏิบัติตาม PDPA หรือไม่ และพิจารณาส่งอีเมลหรือให้นโยบายความเป็นส่วนตัวด้านทรัพยากรบุคคล (HR Privacy Policy) และการตอบรับการยินยอมของผู้สมัครเพื่อดำเนินการแจ้งและขอคำยินยอมจากผู้สมัครงาน • <u>การนำส่งเอกสารสมัครงานที่แผนก HR โดยตรง:</u> พิจารณาส่งนโยบายความเป็นส่วนตัว (Privacy Policy) และมีการกำหนดการ		

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
		ยอมรับฯในส่วนสุดท้ายของแบบฟอร์มสมัครงาน เพื่อบันทึกการยินยอมของผู้สมัครงานก่อนนำส่งเอกสารให้บริษัท 3) ขอคำยินยอมจากผู้ปกครอง กรณีที่บริษัทมีนโยบายรับผู้เยาว์/ยังไม่บรรลุนิติภาวะ เข้าทา งานสำหรับโครงการฝึกงาน เป็นต้น 4) ตรวจสอบให้มั่นใจว่าผู้สมัครงานสามารถเข้าถึงนโยบายความเป็นส่วนตัว (Privacy Policy) ของบริษัทได้โดยง่าย **<u>เอกสารที่จำเป็น:</u>** 1) นโยบายความเป็นส่วนตัว (Privacy Policy) 2) FM-HR-17 : ใบสมัครงาน		
4.	กระบวนการ	**รับใบสมัครที่มีข้อมูลและเอกสารที่เกี่ยวข้อง** **<u>ประเด็น:</u>** เอกสารของผู้สมัครงานไม่ถูกดำเนินการ เนื่องจากบริษัทได้ดำเนินการปิดรับสมัครตำแหน่งงานแล้ว หรือระบบของบริษัทในการรับส่งเอกสารสมัครงานให้หน่วยงานที่เกี่ยวข้องไม่ได้ถูกตั้งค่าอย่างถูกต้อง **<u>ความเสี่ยงด้าน PDPA:</u>** บริษัทมีหน้าที่เก็บรวบรวมข้อมูลส่วนบุคคลที่จำเป็นต่อวัตถุประสงค์ในการสรรหาพนักงาน และมีหน้าที่ป้องกันไม่ให้ข้อมูลสูญหายหรือเปิดเผยต่อบุคคลที่ไม่ได้รับอนุญาต **<u>มาตรการแก้ไข:</u>** ติดตามตรวจสอบการประกาศรับสมัครงานของบริษัทผ่านเว็บไซต์หางานต่างๆ อย่างสม่ำเสมอ เพื่อป้องกันการรับใบสมัครงาน ในตำแหน่งงานที่ปิดรับสมัครไปแล้ว และหลีกเลี่ยงการเก็บรวบรวมข้อมูลส่วนบุคคลที่ไม่จาเป็นและการใช้ข้อมูลส่วนบุคคลอย่างไม่เหมาะสม **<u>เอกสารที่จำเป็น:</u>** นโยบายความเป็นส่วนตัว (Privacy Policy)	HR	6.3.3

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
5.	กระบวนการ	แจ้งผลการปฏิเสธการรับเข้าทางาน **<u>ประเด็น:</u>** ผู้สมัครงานที่ไม่ผ่านการคัดเลือกไม่ทราบถึงสถานะการคัดเลือกของตนเอง **<u>ความเสี่ยงด้าน PDPA:</u>** ผู้สมัครงานที่ไม่ผ่านการคัดเลือกไม่สามารถใช้สิทธิในฐานะเจ้าของข้อมูลได้ เช่น สิทธิในการคัดค้านการเก็บรวบรวม การใช้ และการเปิดเผย สิทธิในการถอนคำยินยอม และสิทธิในการขอให้ลบหรือทำลายข้อมูล (หากเข้าข่าย) เนื่องจากผู้สมัครงานไม่ทราบว่าประวัติของตนจะไม่ถูกนำ ไปพิจารณาต่อ **<u>มาตรการแก้ไข:</u>** 1) ให้บริษัทพิจารณาว่าจะจัดเก็บประวัติส่วนตัวของผู้สมัครงานไว้เพื่อเป็นฐานข้อมูลในการติดต่อผู้สมัครงานรายนี้ หากมีการเปิดตำแหน่งนี้ หรือตำแหน่งอื่นๆ ที่เหมาะสมในอนาคตหรือไม่ 2) หากบริษัทประสงค์ที่จะเก็บประวัติส่วนตัวของผู้สมัครงานรายนี้ไว้ แผนกทรัพยากรบุคคลควรส่งอีเมลแจ้งให้ผู้สมัครงานทราบถึงผลการคัดเลือก เจตนาของบริษัทในการเก็บประวัติส่วนตัวของผู้สมัครงาน ระยะเวลาการเก็บรักษาข้อมูล ตลอดจนสิทธิของผู้สมัครงานในฐานะเจ้าของข้อมูลส่วนบุคคล 3) กำหนดขั้นตอนในการรองรับและบันทึกการใช้สิทธิผู้สมัครงานในฐานะเจ้าของข้อมูลส่วนบุคคลซึ่งการใช้สิทธิของผู้สมัครงานต้องเป็นไปตามฐานทางกฎหมาย 4) หากบริษัทไม่ประสงค์ที่จะเก็บประวัติส่วนตัวของผู้สมัครงานรายนี้ไว้ แผนกทรัพยากรบุคคลควรส่งอีเมลแจ้งให้ผู้สมัครงานทราบถึงผลการคัดเลือก และเจตนาในการลบประวัติส่วนตัวของผู้สมัครงานจากฐานข้อมูลของบริษัท 5) ตรวจสอบให้มั่นใจว่าผู้สมัครงานสามารถเข้าถึงนโยบายความเป็นส่วนตัว (Privacy Policy) ของบริษัทได้โดยง่าย	HR	6.3.4

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
		<u>เอกสารที่จำเป็น:</u> 1) นโยบายความเป็นส่วนตัว (Privacy Policy) 2) PC-MG-13 : นโยบายคุ้มครองข้อมูลส่วนบุคคล (การควบคุมข้อมูลส่วนบุคคล)		
6.	กระบวนการ	**จัดเก็บเอกสารทั้งหมด** **<u>ประเด็น:</u>** การจัดเก็บข้อมูลส่วนบุคคลของผู้สมัครที่ไม่ผ่านการคัดเลือก เกินระยะเวลาที่กฎหมายกำหนดหรือนานเกินความจำเป็น **<u>ความเสี่ยงด้าน PDPA:</u>** 1) บริษัทต้องดำเนินการทำลายข้อมูลส่วนบุคคลของผู้สมัคร เมื่อถึงกำหนดระยะเวลาการเก็บรักษา หรือเมื่อบริษัทไม่มีความจะเป็นที่ต้องใช้ข้อมูลนั้นอีกต่อไป 2) การจัดเก็บเอกสารข้อมูลส่วนบุคคลที่มากและนานเกินความจำเป็น อาจทำให้ประสิทธิภาพของระบบการจัดการเอกสารของบริษัทลดลง ซึ่งจะส่งกระทบต่อมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคลของผู้สมัครในที่สุด **<u>มาตรการแก้ไข:</u>** 1) ทบทวนและแก้ไข (หากจำเป็น) ระยะเวลาจัดเก็บข้อมูลส่วนบุคคลผู้สมัครที่ไม่ผ่านการคัดเลือกให้สอดคล้องกับระยะเวลาที่ทางที่ปรึกษาทางกฎหมายระบุ พร้อมดำเนินการสื่อความการแก้ไขนี้เป็นลายลักษณ์อักษรให้พนักงานแผนกทรัพยากรบุคคลรับทราบ 2) ดำเนินการทำลายข้อมูลขอทั้งไฟล์เอกสารและไฟล์อิเล็กทรอนิกส์อย่างเหมาะสมและตามกำหนดระยะเวลาจัดเก็บข้อมูล โดยการทำลายเอกสารให้ทำเรื่องขอเป็นลายลักษณ์อักษรด้วยเอกสาร FM-DC-01 : ใบขอดำเนินการเอกสาร / DOCUMENT ACTION REQUEST (DAR) และการขอทำลายไฟล์อิเล็กทรอนิกส์ ให้ดำเนินการตามปฏิบัติงาน	HR	6.3.5

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
		SP-IT-03 : การบริหารจัดการข้อมูลฯ 3) จัดให้มีกระบวนการตรวจสอบการลบหรือทำลายข้อมูลของผู้สมัครที่ไม่ผ่านการคัดเลือกว่าเป็นไปตามระยะเวลาที่กำหนดหรือไม่ โดย DPO 4) กำหนดหัวข้อการตรวจสอบแผนกทรัพยากรบุคคลในแผนการปฏิบัติงานของผู้ตรวจสอบภายใน (Internal Audit Plan) เพื่อประเมินประสิทธิภาพของโครงสร้างและผลการปฏิบัติงานกระบวนการเก็บรักษาข้อมูล (Data Retention Process) ของแผนกทรัพยากรบุคคล 5) ตรวจสอบให้มั่นใจว่าผู้สมัครทุกคนสามารถเข้าถึงและรับทราบกระบวนการเก็บรักษาข้อมูลส่วนบุคคล (Data Retention Process) ของบริษัทได้โดยง่าย **<u>เอกสารที่จำเป็น:</u>** 1) FM-DC-01: ใบขอดำเนินการเอกสาร / DOCUMENT ACTION REQUEST (DAR) 2) FM-HR-17: ใบสมัครงาน 3) SP-HR-01: การสรรหาและคัดเลือกพนักงาน 4) SP-IT-03: การบริหารจัดการข้อมูลฯ 5) SP-MG-01: การคุ้มครองข้อมูลส่วนบุคคล 6) PC-MG-13: นโยบายคุ้มครองข้อมูลส่วนบุคคล		
7.	กระบวนการและระบบ	**จัดเก็บเอกสารทั้งหมด** **<u>ประเด็น:</u>** บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงเอกสารส่วนบุคคลของผู้สมัครได้ **<u>ความเสี่ยงด้าน PDPA:</u>** มาตรการคุ้มครองข้อมูลที่ไม่เพียงพออาจทำให้ข้อมูลรั่วไหล และทำให้มีการใช้ และ/หรือประมวลผลข้อมูลส่วนบุคคลของผู้สมัครอย่างไม่เหมาะสมได้	HR / IT	6.3.5

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
		<u>มาตรการแก้ไข:</u> ***การเข้าถึงทางกายภาพ*** 1) ควรจำกัดการเข้าถึงเอกสารข้อมูลส่วนบุคคลของผู้สมัครให้เฉพาะพนักงานที่เกี่ยวข้องเท่านั้น 2) ตรวจสอบให้มั่นใจว่าตู้หรือห้องเก็บเอกสารที่ใช้เก็บข้อมูลส่วนบุคคลและข้อมูลละเอียดอ่อนมีมาตรการรักษาความปลอดภัยที่เหมาะสม เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต 3) กำหนดให้มีกระบวนการในการขอเข้าถึงข้อมูลส่วนบุคคลของผู้สมัครโดยให้ระบุขั้นตอนการปฏิบัติงาน การขออนุมัติ และการบันทึกคำขอที่ชัดเจน รวมถึงระบุผลกระทบที่อาจเกิดขึ้นหากมีการใช้และ/หรือเปิดเผยข้อมูลส่วนบุคคลของผู้สมัครอย่างไม่เหมาะสม 4) หมั่นตรวจสอบและสังเกตการณ์บริเวณพื้นที่ทำงานและหน้าจอคอมพิวเตอร์ของพนักงาน รวมถึงให้มีการจดบันทึกการสังเกตการณ์นั้น เพื่อสนับสนุนให้เกิดวัฒนธรรมที่ดีภายในองค์กรในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ***การเข้าถึงระบบ*** 1) รักษาความปลอดภัยของข้อมูลประจำตัวที่ใช้เข้าถึงบัญชีอีเมล์ของพนักงานในแผนกทรัพยากรบุคคล ระบบบริหารจัดการภายในองค์กรและเว็บไซต์หางาน 2) ป้องกันการถ่ายโอนเอกสารผู้สมัครไปยังอุปกรณ์จัดเก็บข้อมูลแบบพกพา (Portable Storage Devices)ที่ไม่ได้รับอนุญาต โดยการควบคุมการใช้ USB อย่างรัดกุม และให้สิทธิ์เข้าถึงโดยอิงตามบทบาทหน้าที่ของผู้ใช้ 3) ดำเนินการตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit) ของบริษัทอย่างสม่ำเสมอร่วมกับการตรวจสอบภายใน (Internal Audit) เพื่อประเมินความมั่นคงปลอดภัยของโครงสร้างพื้นฐานตรวจจับช่องโหว่ของระบบ และประเมินความเหมาะสมและความเพียงพอของมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ณ ปัจจุบัน 4) เก็บบันทึกการติดตามธุรกรรมของระบบที่ต้องสงสัย รวมถึงการเข้าถึงข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต		

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
		5) ตรวจสอบและแก้ไขสิทธิ์เข้าถึงระบบอย่างสม่ำเสมอ โดยตรวจสอบจากรายชื่อพนักงานและตำแหน่งงานในปัจจุบัน 6) บันทึกกิจกรรมทั้งหมดที่เกิดขึ้นในระบบลงในข้อมูลจราจรทางคอมพิวเตอร์ (Log File) เพื่อเป็นหลักฐานในการตรวจสอบ (Audit Trail) 7) ติดตั้งกล้องวงจรปิดรอบบริเวณที่ต้องรักษาความปลอดภัยและห้องเซิร์ฟเวอร์ในมุมที่เหมาะสม และตรวจสอบการทำงานของกล้องทุกตัวอย่างสม่ำเสมอ 8) กำหนดให้มีเปลี่ยนแปลงรหัสผ่านอย่างสม่ำเสมอ (ทุก 2- 3 เดือน) เพื่อเพิ่มความปลอดภัยของข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในระบบต่าง ๆ **<u>เอกสารที่จำเป็น:</u>** 1) PC-IT-01: นโยบายการรักษาความปลอดภัยสารสนเทศ 2) SP-HR-01: การสรรหาและคัดเลือกพนักงาน		

เอกสารแนบท้าย 6.4) กระบวนการการจ้างพนักงาน การจ่ายผลตอบแทน และการประเมินผลพนักงาน

สรุปความเสี่ยงด้าน PDPA สำหรับกระบวนการว่าจ้างพนักงาน

เนื่องจากขั้นตอนปฏิบัติงานดังกล่าว ไม่ได้มีการจัดทำ แผนผังกระบวนการทำงาน อย่างไรก็ตามได้ระบุสรุปความเสี่ยงด้าน PDPA ที่เกี่ยวกับกระบวนการว่าจ้างพนักงาน รายละเอียดดังต่อไปนี้

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง
1.	กระบวนการและบุคลากร	**ประเด็น:** 1) ขาดการแจ้งข้อมูลเกี่ยวกับจุดประสงค์ในการเก็บรวบรวม ใช้และ/หรือเปิดเผยข้อมูลส่วนตัวแก่พนักงาน 2) ขาดการขอคำยินยอมในการเก็บรวบรวม ข้อมูลส่วนบุคคล/ข้อมูลที่ละเอียดอ่อน (หากจำเป็น) จากพนักงาน **ความเสี่ยงด้าน PDPA:** พนักงานไม่ทราบสิทธิ์ของตนเอง ในฐานะเจ้าของข้อมูลส่วนบุคคล **มาตรการแก้ไข:** จัดอบรมรายละเอียดที่จำเป็นต้องแจ้งให้พนักงานใหม่ทราบในขั้นตอนการปฐมนิเทศ และตรวจสอบให้มั่นใจว่ารายละเอียดที่จำเป็นทั้งหมดได้ถูกระบุไว้ในนโยบายคุ้มครองข้อมูลส่วนบุคคล ของบริษัท เช่น : • วัตถุประสงค์ในการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล • สิทธิของพนักงานในฐานะเจ้าของข้อมูล **เอกสารที่จำเป็น:** 1) PC-MG-13: นโยบายคุ้มครองข้อมูลส่วนบุคคล	HR

สรุปความเสี่ยงด้าน PDPA **สำหรับกระบวนการจ่ายผลตอบแทน ผลประโยชน์และการประเมินผลพนักงาน**

เนื่องจากขั้นตอนปฏิบัติงานดังกล่าว ไม่ได้มีการจัดทำ แผนผังกระบวนการทำงาน อย่างไรก็ตามได้ระบุสรุปความเสี่ยงด้าน PDPA ที่เกี่ยวกับกระบวนการว่าจ้างพนักงาน รายละเอียดดังต่อไปนี้

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง
1.	กระบวนการ	**บันทึกข้อมูลของพนักงานในระบบของบริษัท** **<u>ประเด็น:</u>** การบันทึกข้อมูลที่ไม่ครบถ้วนหรือไม่ถูกต้องของพนักงานเข้าสู่ระบบของบริษัท **<u>ความเสี่ยงด้าน PDPA:</u>** บริษัทมีหน้าที่ตรวจสอบความถูกต้อง เป็นปัจจุบัน ของข้อมูลส่วนบุคคลของพนักงานที่อยู่ในฐานข้อมูลบริษัทเพื่อไม่ทำให้เกิดความเข้าใจผิด **<u>มาตรการแก้ไข:</u>** 1) กำหนดมาตรการรักษาความปลอดภัย (เช่น ขั้นตอนการตรวจสอบและอนุมัติการบันทึกข้อมูลเข้าระบบ) เพื่อให้มั่นใจว่าข้อมูลที่บันทึกเข้าในระบบครบถ้วนและถูกต้อง 2) กำหนดให้มีการสำรวจการเปลี่ยนแปลงข้อมูลส่วนบุคคลของพนักงานเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงข้อมูลส่วนบุคคล 3) กำหนดแผนงานตรวจสอบแผนกทรัพยากรบุคคล รวมอยู่ในแผนการปฏิบัติงานของผู้ตรวจสอบภายใน(Internal Audit Plan) เพื่อประเมินประสิทธิภาพของแนวทางปฏิบัติและผลการปฏิบัติงานในกระบวนการเก็บรักษาข้อมูล (Data Retention Process) ของแผนกทรัพยากรบุคคล **<u>เอกสารที่จำเป็น:</u>** แบบสำรวจการเปลี่ยนแปลงข้อมูลส่วนบุคคลของพนักงาน	HR
2.	กระบวนการและระบบ	**การเก็บรักษาข้อมูลส่วนบุคคลของพนักงาน**	HR/ IT

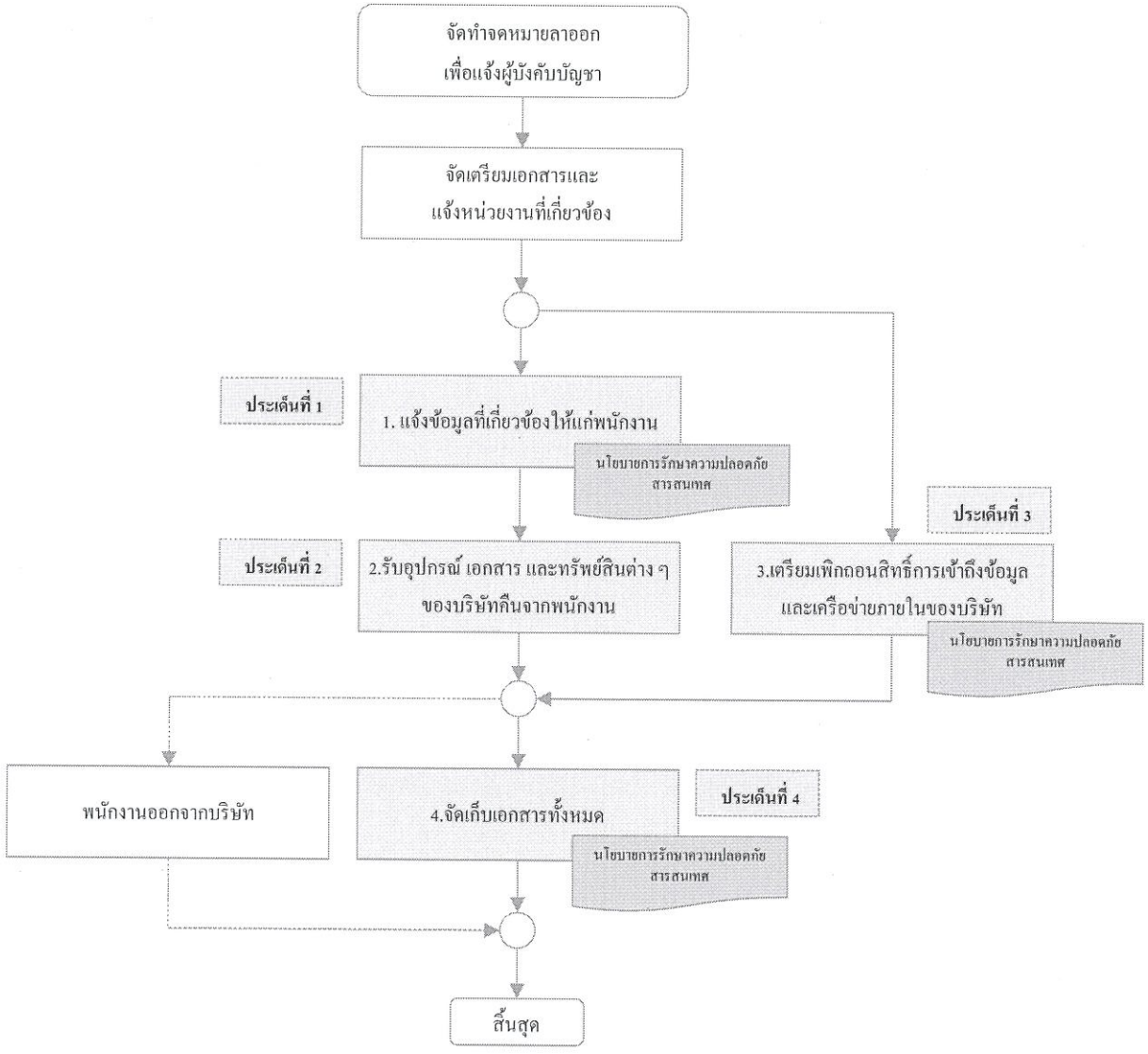
ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง
		<u>ประเด็น:</u> บุคคลที่ได้รับสิทธิ์ในการเข้าถึงข้อมูลในระบบดำเนินการแก้ไขบันทึกข้อมูลของพนักงาน โดยที่พนักงานไม่ได้ขอให้มีการเปลี่ยนแปลงแก้ไขข้อมูล **<u>ความเสี่ยงด้าน PDPA:</u>** มาตรการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพออาจทำให้ข้อมูลสูญหาย รั่วไหล และมีการใช้และ/หรือ ประมวลผลข้อมูลส่วนบุคคลของพนักงานอย่างไม่เหมาะสมได้ **<u>มาตรการแก้ไข:</u>** 1) ตรวจสอบความเหมาะสมและความถูกต้องของโครงสร้างอนุมัติในระบบเป็นประจำทุกปี โดยเทียบกับโครงสร้างการอนุมัติที่กำหนดไว้ในนโยบายของบริษัท เพื่อเป็นมาตรการควบคุมเชิงป้องกัน 2) ตรวจสอบกระบวนการให้สิทธิ์เข้าถึงแก่พนักงาน เพื่อให้มั่นใจว่ามีมาตรการควบคุมที่เหมาะสม 3) จัดทำนโยบายความปลอดภัยทางเทคโนโลยีสารสนเทศ รวมถึงแนวปฏิบัติด้านการบริหารจัดการข้อมูลอย่างมีจริยธรรมและสิทธิ์การเข้าถึง **<u>เอกสารที่จำเป็น:</u>** 1) PC-IT-01: นโยบายการรักษาความปลอดภัยสารสนเทศ 2) SP-IT-03: การบริหารจัดการข้อมูลฯ	
3.	กระบวนการและระบบ	**ยื่นเอกสารของพนักงาน ซึ่งรวมถึงแต่ไม่จำกัดเพียงแค่:** • เอกสารเงินเดือน • ใบรับรองแพทย์ สำเนาสูติบัตร สำเนามรณบัตร/หนังสือรับรองการฝังศพ เพื่อเป็นเอกสารประกอบการขอลาหยุด • เอกสารการเบิกเงิน เช่น ค่ารักษาพยาบาล ค่าที่พัก/ค่าล่วงเวลาและค่าเบี้ยเลี้ยงเดินทาง • บันทึกการเข้า-ออกงาน/การทำงานล่วงเวลา	HR/ IT

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง
		• บันทึกการฝึกอบรมในหรือนอกบริษัท • บันทึกการประเมินผลการปฏิบัติงานของพนักงาน **ประเด็น:** บุคคลภายนอกสามารถเข้าถึงข้อมูลส่วนบุคคลของพนักงาน โดยไม่ได้รับอนุญาต **ความเสี่ยงด้าน PDPA:** มาตรการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพออาจทำให้ข้อมูลสูญหาย รั่วไหล และมีการใช้และ/หรือประมวลผลข้อมูลส่วนบุคคลของพนักงานอย่างไม่เหมาะสมได้ **มาตรการแก้ไข:** 1) ควรจำกัดการเข้าถึงเอกสารข้อมูลส่วนบุคคลของพนักงานให้เฉพาะพนักงานแผนกทรัพยากรบุคคลที่เกี่ยวข้องเท่านั้น 2) กำหนดให้มีกระบวนการในการขอเข้าถึงข้อมูลส่วนบุคคลของพนักงาน โดยต้องได้รับการอนุมัติจากผู้มีอำนาจ 3) ตรวจสอบให้มั่นใจว่าตู้หรือห้องเก็บเอกสารที่ใช้เก็บข้อมูลส่วนบุคคลและข้อมูลละเอียดอ่อนมีมาตรการรักษาความปลอดภัยที่เหมาะสม เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต 4) อัปเดตซอฟต์แวร์รักษาความปลอดภัยอยู่เสมอ เพื่อยกระดับมาตรการรักษาความปลอดภัยและเป็นการป้องกันภัยคุกคามทางไซเบอร์ (Cyber Attack) 5) ตรวจสอบและแก้ไขสิทธิ์เข้าถึงระบบอย่างสม่ำเสมอ โดยตรวจสอบจากรายชื่อพนักงานและตำแหน่งงานในปัจจุบัน **เอกสารที่จำเป็น:** PC-IT-01: นโยบายการรักษาความปลอดภัยสารสนเทศ	

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง
4.	กระบวนการ	**ยื่นเอกสารของพนักงาน ซึ่งรวมถึงแต่ไม่จำกัดเพียงแค่:** • เอกสารเงินเดือน • ใบรับรองแพทย์ สำเนาสูติบัตร สำเนามรณบัตร/หนังสือรับรองการฝังศพ เพื่อเป็นเอกสารประกอบการขอลาหยุด • เอกสารการเบิกเงิน เช่น ค่ารักษาพยาบาล ค่าที่พัก/ค่าล่วงเวลาและค่าเบี้ยเลี้ยงเดินทาง • บันทึกการเข้า-ออกงาน/การทางานล่วงเวลา • บันทึกการฝึกอบรมในหรือนอกบริษัท • บันทึกการประเมินผลการปฏิบัติงานของพนักงาน **<u>ประเด็น:</u>** การจัดเก็บข้อมูลส่วนบุคคลของพนักงาน เกินระยะที่จัดเก็บหรือจัดเก็บนานเกินความจำเป็น โดยไม่มีการทบทวนระยะเวลาการจัดเก็บ **<u>ความเสี่ยงด้าน PDPA:</u>** การเก็บรักษาข้อมูลส่วนบุคคลนานกว่าที่นโยบายการเก็บรักษาข้อมูลหรือข้อกำหนดในการเก็บรักษาข้อมูลที่PDPA กำหนด สามารถนำไปสู่ 1) การจัดเก็บข้อมูลส่วนบุคคลของพนักงานที่ไม่มีความเคลื่อนไหวหรืออดีตพนักงาน โดยไม่ได้รับอนุญาต 2) การสูญเสียความสมบูรณ์ของข้อมูลที่เกิดจากการประมวลผลข้อมูลส่วนบุคคลของพนักงานที่ล้าสมัย 3) การใช้และ/หรือการประมวลผลข้อมูลส่วนบุคคลของพนักงานที่ไม่เหมาะสม **<u>มาตรการแก้ไข:</u>** 1) กำหนดให้มีกระบวนการตรวจสอบความถูกต้องของข้อมูลพนักงานทั้งพนักงานปัจจุบันและพนักงานที่พ้นสภาพแล้ว และปรับปรุงข้อมูลให้เป็นปัจจุบันเพื่อให้สอดคล้องกับวัตถุประสงค์ในการเก็บรวบรวมข้อมูล	HR

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง
		2) กำหนดระยะเวลาในการทบทวนข้อมูลส่วนบุคคลของพนักงาน เพื่อตรวจสอบให้มั่นใจว่าข้อมูลของพนักงานมีความเป็นปัจจุบัน และข้อมูลของพนักงานที่พ้นสภาพได้ถูกลบในระยะเวลาที่กำหนด 3) จัดทำแผนการทบทวนข้อมูลส่วนบุคคลและทำการปรับปรุงแก้ไขเพื่อให้สอดคล้องกับกฎหมาย รวมถึงให้มีการบันทึกกิจกรรมนั้นอย่างเหมาะสมและเป็นหมวดหมู่ 4) แจ้งให้พนักงานและผู้ที่รับผิดชอบทราบถึงกระบวนการเก็บรักษาข้อมูล (Retention Process) และการดำเนินการเพื่อให้มั่นใจว่ามีการปฏิบัติเป็นไปตามกำหนดระยะเวลาเก็บรักษาข้อมูล (Retention Schedule) 5) กำหนดมาตรการควบคุมที่เหมาะสมและเพียงพอในการบันทึกกิจกรรมการลบข้อมูลลูกค้าจากที่ไฟล์จัดเก็บเอกสาร ฐานข้อมูล และเซิร์ฟเวอร์ที่ใช้สำรองข้อมูลของบริษัท 6) ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อนควรถูกลบอย่างเหมาะสมด้วยวิธีการที่รัดกุมกว่าข้อมูลส่วนบุคคลเพื่อให้มั่นใจว่าข้อมูลเหล่านั้นจะไม่ถูกกู้คืนและนำกลับมาใช้งานต่อได้อีก 7) กำหนดให้คณะกรรมการตรวจสอบภายใน และ DPO มีการตรวจสอบกระบวนการลบทำลายข้อมูลส่วนบุคคล เพื่อให้มั่นใจว่าข้อมูลส่วนบุคคลของพนักงานจะถูกลบออกจากฐานข้อมูลของบริษัทเมื่อสิ้นสุดระยะเวลาการเก็บรักษา **<u>เอกสารที่จำเป็น:</u>** 1) PC-IT-01 : นโยบายการรักษาความปลอดภัยสารสนเทศ 2) SP-HR-01 : การสรรหาและการคัดเลือก	

เอกสารแนบท้าย **6.5) กระบวนการลาออกของพนักงาน**



สรุปความเสี่ยงด้าน PDPA สำหรับกระบวนการลาออกของพนักงาน

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
1.	กระบวนการ	**แจ้งข้อมูลที่เกี่ยวข้องให้แก่พนักงาน** **<u>ประเด็น:</u>** พนักงานที่อยู่ระหว่างการดำเนินเรื่องลาออกไม่ทราบว่าข้อมูลส่วนบุคคลอะไรบ้างของตนเองจะยังถูกเก็บไว้เป็นเวลานานเท่าใด ภายหลังจากที่ได้ลาออกไปแล้ว **<u>ความเสี่ยงด้าน PDPA:</u>** บริษัทมีหน้าที่แจ้งระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคลที่ชัดเจนให้พนักงานรับทราบ ตลอดจนสิทธิของพนักงานในฐานะเจ้าของข้อมูลส่วนบุคคล **<u>มาตรการแก้ไข:</u>** 1) ยืนยันความถูกต้องของข้อมูลของพนักงาน เพื่อประโยชน์ในการใช้อ้างอิงข้อมูลในอนาคต 2) จัดทำรายการตรวจสอบ (Checklist) ที่ระบุรายละเอียดที่ต้องแจ้งแก่พนักงานที่ประสงค์จะลาออก 3) กำหนดขั้นตอนเพื่อรองรับและบันทึก ในกรณีที่พนักงานที่ประสงค์ลาออกขอใช้สิทธิในฐานะเจ้าของข้อมูล (เช่น สิทธิ์ในการลบข้อมูล และสิทธิ์ในการคัดค้าน) ทั้งนี้การขอใช้สิทธินั้นต้องเป็นไปตามข้อกำหนดโดยชอบด้วยกฎหมาย 4) กำหนดกระบวนการตรวจสอบการดำเนินการตามคำขอของพนักงานที่ประสงค์ลาออก 5) แจ้งให้พนักงานที่ประสงค์ลาออกรับทราบ เมื่อได้ดำเนินการแล้วเสร็จตามคำขอใช้สิทธิของพนักงาน ในฐานะเจ้าของข้อมูลส่วนบุคคล 6) ตรวจสอบให้มั่นใจว่าพนักงานทุกคนสามารถเข้าถึงนโยบายความเป็นส่วนตัว (Privacy Policy) ของบริษัทได้โดยง่าย และกระบวนการเก็บรักษาข้อมูล (Data Retention Process)	HR	6.5.1

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
		<u>เอกสารที่จำเป็น:</u> 1) PC-IT-01: นโยบายการรักษาความปลอดภัยสารสนเทศ 2) SP-HR-01: การสรรหาและคัดเลือกพนักงาน		
2.	กระบวนการ	**รับอุปกรณ์ เอกสาร และทรัพย์สินต่าง ๆ ของบริษัทคืนจากพนักงาน** **<u>ประเด็น:</u>** บุคคลที่พ้นสภาพการเป็นพนักงานยังคงสามารถเข้าถึงทรัพย์สินและข้อมูลที่เป็นความลับของบริษัทได้ **<u>ความเสี่ยงด้าน PDPA:</u>** การที่บุคคลที่พ้นสภาพการเป็นพนักงานสามารถเข้าถึงข้อมูลและทรัพย์สินของบริษัทได้ สามารถก่อให้เกิดการละเมิดความปลอดภัย การรั่วไหลของข้อมูล และการใช้และ/หรือประมวลผลข้อมูลส่วนบุคคลอย่างไม่เหมาะสมได้ **<u>มาตรการแก้ไข:</u>** 1) จัดทำรายการตรวจสอบ (Checklist) สินทรัพย์ทางกายภาพและสินทรัพย์ที่ไม่มีลักษณะทางกายภาพ (เช่น กุญแจ คีย์การ์ด ไฟล์เอกสาร แล็ปท็อป ข้อมูลลูกค้าและข้อมูลบริษัท) ที่แผนกทรัพยากรบุคคลต้องดำเนินการเรียกคืนจากพนักงาน 2) ตรวจสอบการลงนามร่วมกันของพนักงานที่ประสงค์ลาออก แผนกทรัพยากรบุคคล และแผนกเทคโนโลยีสารสนเทศ ในรายการตรวจสอบทรัพย์สินในขั้นตอนที่ 1 ข้างต้น เมื่อพนักงานที่ประสงค์ลาออกได้ดำเนินการคืนอุปกรณ์และทรัพย์สินของบริษัทเรียบร้อยแล้ว 3) แจ้งวันลาออกที่มีผลบังคับใช้ให้แผนกเทคโนโลยีสารสนเทศรับทราบ เพื่อให้มีดำเนินการยุติการเข้าถึงข้อมูล/ระบบ เมื่อพนักงานพ้นสภาพอย่างทันท่วงที	HR / IT	6.5.2

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
		<u>เอกสารที่จำเป็น:</u> 1) FM-HR-23: รายการทรัพย์สินของบริษัทฯที่พนักงานต้องคืนเมื่อลาออก-พ้นสภาพจากการเป็นพนักงานบริษัท 2) FM-IT-04: แบบฟอร์มการถอนสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ 3) SP-HR-04: การพ้นสภาพการว่าจ้าง		
3.	กระบวนการและระบบ	**เตรียมเพิกถอนสิทธิ์การเข้าถึงข้อมูลและเครือข่ายภายในของบริษัท** **<u>ประเด็น:</u>** บุคคลที่พ้นสภาพการเป็นพนักงานของบริษัทยังคงสามารถเข้าถึงเครือข่าย/ระบบภายในของบริษัท **<u>ความเสี่ยงด้าน PDPA:</u>** การที่บุคคลที่พ้นสภาพการเป็นพนักงานสามารถเข้าถึงข้อมูลและทรัพย์สินของบริษัทได้ สามารถก่อให้เกิดการละเมิดความปลอดภัย การรั่วไหลของข้อมูล และการใช้และ/หรือประมวลผลข้อมูลส่วนบุคคลอย่างไม่เหมาะสมได้ **<u>มาตรการแก้ไข:</u>** 1) ตรวจสอบให้แน่ใจว่าสิทธิ์เข้าถึงทั้งหมด เช่น อีเมล์ เครือข่ายของบริษัท และสิทธิ์เข้าถึงจากระยะไกล (Remote Access) ที่มอบให้แก่พนักงานได้ถูกเพิกถอนโดยสมบูรณ์ เมื่อพนักงานพ้นสภาพแล้ว 2) กำหนดกระบวนการตรวจสอบเพื่อบันทึกขั้นตอนการยกเลิกสิทธิ์เข้าถึง เพื่อบันทึกรายละเอียดวันที่สิ้นสุดการเข้าถึงชื่อของพนักงาน แผนกเทคโนโลยีสารสนเทศซึ่งเป็นผู้ดำเนินการยกเลิกสิทธิ์และชื่อผู้ตรวจสอบก่อนส่งหลักฐานการตรวจสอบให้แผนกทรัพยากรบุคคลจัดเก็บ 3) ดำเนินการตรวจสอบภายในเป็นระยะ ๆ เพื่อให้มั่นใจว่าได้มีการยกเลิกสิทธิ์การเข้าถึงของพนักงานที่ลาออกไปแล้วอย่างทันท่วงที	IT	6.5.3

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
		4) ระบุขั้นตอนการปฏิบัติงานในการยกเลิกสิทธิ์เข้าถึงเครือข่ายนโยบายการรักษาความปลอดภัยสารสนเทศ และระเบียบปฏิบัติงานการขอใช้บริการงานเทคโนโลยีสารสนเทศ **<u>เอกสารที่จำเป็น:</u>** 1) PC-IT-01 : นโยบายการรักษาความปลอดภัยสารสนเทศ 2) SP-IT-01 : การขอใช้บริการงานเทคโนโลยีสารสนเทศ		
4.	กระบวนการและระบบ	**จัดเก็บเอกสารทั้งหมด** **<u>ประเด็น:</u>** บุคคลภายนอกสามารถเข้าถึงข้อมูลของบุคคลที่พ้นสภาพการเป็นพนักงานโดยไม่ได้รับอนุญาต **<u>ความเสี่ยงด้าน PDPA:</u>** มาตรการคุ้มครองข้อมูลส่วนบุคคลที่ไม่เพียงพออาจทำให้ข้อมูลสูญหาย รั่วไหล และมีการใช้และ/หรือ ประมวลผลข้อมูลส่วนบุคคลของพนักงานอย่างไม่เหมาะสมได้ **<u>มาตรการแก้ไข:</u>** *การเข้าถึงทางกายภาพ* 1) ควรจำกัดการเข้าถึงเอกสารข้อมูลส่วนบุคคลของพนักงานให้เฉพาะพนักงานแผนกทรัพยากรบุคคลที่เกี่ยวข้องเท่านั้น 2) ตรวจสอบให้มั่นใจว่าตู้หรือห้องเก็บเอกสารที่ใช้เก็บข้อมูลส่วนบุคคลและข้อมูลละเอียดอ่อน มีมาตรการรักษาความปลอดภัยที่เหมาะสม เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต 3) กำหนดให้มีกระบวนการในการขอเข้าถึงข้อมูลส่วนบุคคลของพนักงาน โดยให้ระบุขั้นตอนการปฏิบัติงาน การขออนุมัติ และการบันทึกคำขอที่ชัดเจน รวมถึงระบุผลกระทบที่อาจเกิดขึ้นหากมีการใช้และ/หรือเปิดเผยข้อมูลส่วนบุคคลของพนักงานอย่างไม่เหมาะสม	HR / IT	6.5.4

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
		4) หมั่นตรวจสอบและสังเกตการณ์บริเวณพื้นที่ทำงานและหน้าจอคอมพิวเตอร์ของพนักงาน รวมถึงให้มีการจดบันทึกการสังเกตการณ์นั้น เพื่อสนับสนุนให้เกิดวัฒนธรรมที่ดีภายในองค์กรในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ***การเข้าถึงระบบ*** 1) รักษาความปลอดภัยของข้อมูลประจำตัวที่ใช้เข้าถึงบัญชีอีเมลของพนักงานฝ่ายทรัพยากรบุคคล และระบบบริหารจัดการภายในองค์กร 2) ป้องกันการถ่ายโอนเอกสารของพนักงานไปยังอุปกรณ์จัดเก็บข้อมูลแบบพกพา (Portable Storage Devices) ที่ไม่ได้รับอนุญาต โดยการควบคุมการใช้ USB อย่างรัดกุม และให้สิทธิ์เข้าถึงโดยอิงตามบทบาทหน้าที่ของผู้ใช้ 3) ดำเนินการตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit) ของบริษัทอย่างสม่ำเสมอร่วมกับการตรวจสอบภายใน (Internal Audit) เพื่อประเมินความมั่นคงปลอดภัยของโครงสร้างพื้นฐานตรวจจับช่องโหว่ของระบบ และประเมินความเหมาะสมและความเพียงพอของมาตรการรักษาความปลอดภัยของข้อมูลส่วนบุคคล ณ ปัจจุบัน 4) เก็บบันทึกการติดตามธุรกรรมของระบบที่ต้องสงสัย รวมถึงการเข้าถึงข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต 5) ตรวจสอบและแก้ไขสิทธิ์เข้าถึงระบบอย่างสม่ำเสมอ โดยตรวจสอบจากรายชื่อพนักงานและตำแหน่งงานในปัจจุบัน 6) บันทึกกิจกรรมทั้งหมดที่เกิดขึ้นในระบบลงในข้อมูลจราจรทางคอมพิวเตอร์ (Log File) เพื่อเป็นหลักฐานในการตรวจสอบ (Audit Trail)[1] 7) ติดตั้งกล้องวงจรปิดรอบบริเวณที่ต้องรักษาความปลอดภัยและห้องเซิร์ฟเวอร์ในมุมที่เหมาะสม และตรวจสอบการทำงานของกล้องทุกตัวอย่างสม่ำเสมอ 8) กำหนดให้มีเปลี่ยนแปลงรหัสผ่านอย่างสม่ำเสมอ (ทุก 2-3 เดือน) เพื่อเพิ่มความปลอดภัยของข้อมูลส่วนบุคคลที่ถูกเก็บรวบรวมในระบบต่างๆ		

ประเด็นที่	ประเภทประเด็น	กิจกรรมที่ได้รับผลกระทบจาก PDPA	หน่วยงานที่เกี่ยวข้อง	เลขที่อ้างอิงของผัง
		<u>เอกสารที่จำเป็น:</u> 1) PC-IT-01 : นโยบายการรักษาความปลอดภัยสารสนเทศ 2) SP-HR-01 : การสรรหาและคัดเลือกพนักงาน		