นโยบายคุ้มครองข้อมูลส่วนบุคคล

คณะกรรมการของบริษัทเห็นถึงความสำคัญ ในการประมวลผลข้อมูลส่วนบุคคลให้เหมาะสมและถูกต้องตามกฎหมาย คณะกรรมการบริษัท จึงได้มีมติอนุมัติรับรองและออกประกาศบริษัทเรื่อง นโยบายคุ้มครองข้อมูลส่วนบุคคล ฉบับนี้ขึ้น เพื่อกำหนดกรอบ การประมวลผลข้อมูลส่วนบุคคลในกระบวนการต่างๆของบริษัท ไม่ให้กระทบสิทธิของเจ้าของข้อมูลมากเกินไป โดยรับประกันให้ เป็นไปตามนโยบายการกำกับดูแลและบริหารจัดการการประมวลผลข้อมูลดังกล่าว ให้ถูกต้องตามมาตรฐานที่ระบุไว้โดยหน่วยงานกำกับดูแล และเพื่อให้พนักงานและบุคคลที่เกี่ยวข้องของบริษัทยึดถือและปฏิบัติตามให้เป็นไปตามพระราชบัญญัติคุ้มครอง ข้อมูลส่วนบุคคล พ.ศ. 2562 (“พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล”) และมาตรฐานที่กำหนดไว้

ข้อ 1 ประกาศและผลบังคับใช้ของประกาศ

ประกาศฉบับนี้เรียกว่า“นโยบายคุ้มครองข้อมูลส่วนบุคคล” โดยให้มีผลบังคับใช้ตั้งแต่วันที่ 1 พฤษภาคม 2564 เป็นต้นไป

ข้อ 2 คู่มือและคำแนะนำในการปฏิบัติตามประกาศ

โดยอาศัยอำนาจของประกาศบริษัทฉบับนี้ บริษัทอาจพิจารณากำหนดและประกาศคู่มือการปฏิบัติงานโดยละเอียด เพื่อกำหนดแนวทางการปฏิบัติต่างๆ ด้วยจุดประสงค์รับประกันความสมบูรณ์ ถูกต้อง และครบถ้วนในการคุ้มครองข้อมูลส่วนบุคคลให้ถูกต้องเพิ่มเติม โดยให้คู่มือการปฏิบัติงานดังกล่าวมีผลบังคับสมบูรณ์เช่นเดียวกันกับประกาศฉบับนี้

ข้อ 3 โครงสร้างการบริหารจัดการและกำกับการประมวลผลข้อมูลส่วนบุคคล

เพื่อให้การกำกับดูแลและบริหารจัดการด้านการคุ้มครองการประมวลผลข้อมูลส่วนบุคคล ให้สมบูรณ์ถูกต้องสอดคล้องกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล บริษัทกำหนดจัดตั้งโครงสร้างดังต่อไปนี้

3.1. คณะกรรมการบริษัท มีหน้าที่รับผิดชอบในการกำหนดทิศทางและการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลในภาพรวมของบริษัทและบริหารจัดการความเสี่ยงต่างๆ ที่อาจเกิดจากการประมวลผลข้อมูลส่วนบุคคล โดยมีบทบาทหลักในการตรวจสอบและอนุมัติทุกนโยบายย่อยและคู่มือแนวทางการปฏิบัติที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคล

3.2. ประธานเจ้าหน้าที่ฝ่ายบริหาร (CEO) รับผิดชอบโดยตรงในการกำกับดูแลการปฏิบัติงานการประมวลผลข้อมูลส่วนบุคคลโดยรวมของบริษัทผ่านการกำกับดูแลและการรายงานของหัวหน้าหน่วยงานหรือผู้จัดการฝ่ายที่เกี่ยวข้องภายใต้การมอบหมายและการชี้นำของคณะกรรมการบริษัท

3.3. เพื่อการกำกับดูแลการปฏิบัติงานประมวลผลข้อมูลส่วนบุคคลให้ถูกต้องตามนโยบายและกฎหมาย บริษัทได้กำหนดการประมวลผลข้อมูลส่วนบุคคลภายใต้รูปแบบโครงสร้าง 3 Lines of Defense ดังนี้

- 1st Line of Defense: Risk Owner ได้แก่ ประธาน หรือหัวหน้าฝ่าย/หน่วยงาน ซึ่งมีหน้าที่รับผิดชอบ โดยตรงในการกำกับดูแลการประมวลผลข้อมูลส่วนบุคคลของพนักงานภายในหน่วยงานของตน ให้ถูกต้องและสอดคล้องกับนโยบายและกฎหมายที่เกี่ยวข้อง โดยเฉพาะ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล

- 2nd Line of Defense: Risk Control กำหนดให้มีการแต่งตั้งคณะทำงานคุ้มครองข้อมูลส่วนบุคคล (Data Protection Working Committee) ซึ่งประกอบด้วยหัวหน้าฝ่ายที่มีการประมวลผลข้อมูลส่วนบุคคลต่างๆ ในบริษัท ทำงานร่วมกับหน่วยงานกำกับดูแลการปฏิบัติงาน (Compliance) โดยการทำงานของคณะกรรมการ มีความเป็นไปอิสระภายใต้หลักการ maker-checker ดังนั้น กรณีการตรวจสอบการทำงานฝ่ายงานใด หัวหน้าฝ่ายงานดังกล่าวย่อมไม่มีสิทธิในการแทรกแซงหรือให้คำแนะนำใด โดยให้ดำเนินการรายงานโดยตรงไปยัง ประธานเจ้าหน้าที่ฝ่ายบริหาร
- 3rd Line of Defense: Risk Assurance ได้แก่ คณะกรรมการตรวจสอบ (Audit Committee) ซึ่งมีหน้าที่กำกับดูแลและตรวจสอบการดำเนินการประมวลผลข้อมูลส่วนบุคคลของทุกหน่วยงานอีก

3.4. บริษัทกำหนดให้มีการจัดสรรทรัพยากรอย่างเพียงพอ ในการสนับสนุนการปฏิบัติงานของแต่ละหน่วยงานให้เป็นไปตามนโยบายและมาตรฐานการคุ้มครองการประมวลผลข้อมูลส่วนบุคคลในทุกส่วน โดยจัดให้มีทรัพยากรที่จำเป็น ทั้งในแง่ของระบบงานบุคลากร และงบประมาณ

ข้อ 4 การประเมินและบริหารจัดการความเสี่ยงการประมวลผลข้อมูลส่วนบุคคล

4.1. บริษัทกำหนดให้มีการประเมินความเสี่ยงการประมวลผลข้อมูลส่วนบุคคล เพื่อตรวจสอบความพร้อมและความถูกต้อง ในการประมวลผลข้อมูลตามกฎหมายในภาพรวมขององค์กร (Enterprise Risk Management) อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงที่เพิ่มเติมรูปแบบการประมวลผลข้อมูลส่วนบุคคลจากที่ได้ประเมินไว้ภายใต้หลักการที่กำหนดให้แต่ละหน่วยงานที่เกี่ยวข้องในโครงสร้างการกำกับดูแล มีหน้าที่และความรับผิดชอบในกระบวนการประเมินการบริหารจัดการความเสี่ยงในการประมวลผลข้อมูลส่วนบุคคลภายในหน่วยงานของตน รวมถึง การติดตามและรายงานผลด้านความเสี่ยงให้แก่หน่วยงานกำกับดูแลตามที่กำหนดไว้และรายงานต่อคณะกรรมการบริษัท

4.2. บนพื้นฐานการประเมินความเสี่ยงในระดับองค์กร สำหรับการประมวลผลข้อมูลส่วนบุคคลที่มีความเสี่ยงสูงที่จะมีผลกระทบถึงสิทธิเสรีภาพของบุคคล ซึ่งอาจนำไปสู่การเสียประโยชน์ทางเศรษฐกิจและสังคมอย่างมีนัย สำคัญของเจ้าของข้อมูลส่วนบุคคล หรือที่จะทำให้เจ้าของข้อมูลไม่สามารถควบคุมข้อมูลส่วนบุคคลของตนได้ บริษัทกำหนดให้มีการจัดทำการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคลหรือ Data Processing Impact Assessment เพิ่มขึ้น ก่อนการตัดสินใจดำเนินการประมวลผลข้อมูลส่วนบุคคลกรณีดังกล่าว

4.3. ในการประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล บริษัทดำเนินการภายใต้หลักการ ดังนี้

1) มีการอธิบายรายละเอียดการประมวลผลข้อมูลดังกล่าว ซึ่งระบุถึงขอบเขตการประเมินผล วัตถุประสงค์ความจำเป็นในการประมวลผลข้อมูลดังกล่าว

2) มีกระบวนการปรึกษาหารือกับผู้มีส่วนเกี่ยวข้องต่างๆ ได้แก่ เจ้าของข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลที่เกี่ยวข้อง โดยจัดทำกระบวนการปรึกษาหารือทั้งภายในและภายนอกองค์กร
3) มีคำอธิบายที่ชัดเจนเกี่ยวกับความจำเป็นและความได้สัดส่วนของการประมวลผลข้อมูล
4) จัดให้มีการประเมินความเสี่ยงที่จะส่งผลกระทบต่อสิทธิเสรีภาพของเจ้าของข้อมูลโดยคำนึงถึง “ความน่าจะเป็น” (likelihood) และ “ความรุนแรงของผลกระทบ” (severity)
5) รายละเอียดมาตรการในการลดความเสี่ยงที่ระบุไว้ ทั้งนี้ มีการจดบันทึกและจัดทำรายงานการประเมินอย่างเป็นขั้นตอน

ข้อ 5 การสื่อสารประชาสัมพันธ์นโยบาย

บริษัทให้ความสำคัญต่อการสื่อสารนโยบายและแนวทางการปฏิบัติงานที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลให้แก่พนักงานของบริษัท โดยได้มีการสื่อสารผ่านทุกช่องทางการติดต่อกับพนักงาน โดยเฉพาะเมื่อมีการเปลี่ยนแปลงที่มีสาระสำคัญและกระทบต่อการประมวลผลข้อมูลส่วนบุคคลรวมของบริษัท

ข้อ 6 การกำกับดูแลและตรวจสอบ

บริษัทได้กำหนดให้มีการติดตามและตรวจสอบการปฏิบัติตามนโยบายการประมวลผลข้อมูลส่วนบุคคลภายใต้หลักการดังนี้

6.1. กำหนดให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคล ทำหน้าที่หลักในการติดตามและตรวจสอบการปฏิบัติตามนโยบายและมาตรการการประมวลผลข้อมูลส่วนบุคคล และมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่บริษัทกำหนด และการรายงานผลการติดตามและตรวจสอบต่อประธานเจ้าหน้าที่ฝ่ายบริหาร และรายงานต่อคณะกรรมการบริษัท อย่างน้อยปีละ 1 ครั้ง หรือกรณีมีการละเมิดอย่างมีนัยสำคัญต่อธุรกิจ หรือชื่อเสียงของบริษัท
6.2. กำหนดให้มีแผนการตรวจสอบด้านการประมวลผลข้อมูลส่วนบุคคลของบริษัท พร้อมทั้งรายงานผลการตรวจสอบด้านความเสี่ยงต่อคณะกรรมการบริษัทอย่างน้อยปีละ 1 ครั้ง หรือ ทุกครั้งที่มีการเปลี่ยนแปลงอันสำคัญในบริษัท
6.3. กรณีที่ตรวจพบการฝ่าฝืนนโยบายและมาตรการการคุ้มครองการประมวลผลข้อมูลส่วนบุคคล คณะทำงานคุ้มครองข้อมูลส่วนบุคคลจะเป็นหน่วยงานรับเรื่องร้องเรียน กำกับดูแลหลัก รวมถึงทำหน้าที่ตรวจสอบจนทราบข้อเท็จจริง หากพบว่าเกิดการฝ่าฝืนหรือละเมิดนั้นจริง คณะทำงานจะเสนอไปยังประธานเจ้าหน้าที่ฝ่ายบริหาร (CEO) หรือกรรมการ แล้วแต่ความรุนแรงของการละเมิด และตำแหน่งของผู้ที่กระทำผิดเพื่อพิจารณากำหนดมาตรการลงโทษตามข้อกำหนดที่ระบุไว้ ตามการลงโทษทางวินัยตามระเบียบบริหารงานบุคคลต่อไป

ข้อ 7 การจัดทำบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล (Report of Processing) และนโยบายการเปิดเผยข้อมูลส่วนบุคคลให้แก่หน่วยงานภายนอก (Information Disclosure Policy)

บริษัทกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการข้อมูลส่วนบุคคล โดยจัดระดับความลับของข้อมูลดังกล่าวเป็น “ข้อมูลความลับที่สุด (Strictly Confidential)” ภายใต้หลักการในการรักษาความลับของบริษัท โดยดำเนินการบริหารจัดการข้อมูลดังกล่าวภายใต้หลักการ ดังนี้

7.1. กำหนดให้แต่ละฝ่ายงานหรือหน่วยงานที่มีหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลเป็นผู้รับผิดชอบในการจัดทำบันทึกรายการประมวลผลข้อมูลส่วนบุคคล และปรับปรุงรายการการประมวลผลข้อมูลดังกล่าวอย่างสม่ำเสมอ รวมทั้งระบุข้อกำหนดในการประมวลผลข้อมูลส่วนบุคคลให้พนักงานภายในฝ่ายงานของตนรับทราบ เพื่อให้มั่นใจว่า พนักงานดังกล่าวตระหนักรู้ถึงความสำคัญของสิทธิของเจ้าของข้อมูล รวมถึงหน้าที่ในการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งหมดนั้น

7.2. บริษัทกำหนดนโยบายให้การประมวลผลข้อมูลส่วนบุคคลทั้งหมดดำเนินการผ่านระบบอิเล็กทรอนิกส์ ที่ควบคุมการเข้าถึงและบันทึกการเข้าถึงได้มากกว่าการจัดเก็บข้อมูลเป็นกระดาษ ในกรณีใช้ข้อมูลส่วนบุคคลในรูปแบบของกระดาษ ได้มีการจัดทำบันทึกการใช้ข้อมูลและมีนโยบาย Clean Desk โดยห้ามนำกระดาษที่มีข้อมูลส่วนบุคคลไปใช้ซ้ำ (Recycled) และกำหนดให้มีการจัดเก็บใส่กล่องให้เรียบร้อยและกำหนดระยะเวลาการเก็บข้อมูลดังกล่าว และหากมีการเคลื่อนย้ายข้อมูลดังกล่าว ได้กำหนดให้มีการดำเนินการตามกระบวนการรักษาความมั่นคงปลอดภัยของข้อมูล

7.3. ในกรณีที่มีความจำเป็นต้องส่งต่อหรือเปิดเผยข้อมูลส่วนบุคคลให้แก่บุคคลภายนอกองค์กร บริษัทได้กำหนดให้มีการดำเนินการ ดังนี้

- มีการตรวจสอบความจำเป็น รวมถึงความเสี่ยงในการส่งต่อข้อมูลส่วนบุคคลและความน่าเชื่อถือของผู้รับข้อมูลส่วนบุคคลดังกล่าวก่อน
- การส่งต่อหรือเปิดเผยแต่ละครั้งต้องได้รับความยินยอมจากผู้บังคับบัญชาตามอำนาจการอนุมัติ
- กำหนดให้พนักงานทุกคน และทุกหน่วยงานมีหน้าที่การบันทึกรายการการประมวลผลข้อมูลส่วนบุคคล การส่งต่อเปิดเผยข้อมูลออกไปนอกองค์กรดังกล่าว
- พนักงานผู้เปิดเผยหรือส่งต่อข้อมูล ต้องปฏิบัติตามช่องทางและวิธีการส่งต่อหรือเปิดเผยข้อมูลที่บริษัท กำหนดเพื่อให้มีความเสี่ยงด้านความมั่นคงปลอดภัยน้อยที่สุด รวมถึงหลีกเลี่ยงการส่งผ่านช่องทางส่วนตัวที่ไม่สามารถควบคุมได้
- กำหนดให้มีการลงนามในสัญญา หรือข้อตกลงการประมวลผลข้อมูลส่วนบุคคลระหว่างบริษัทและบุคคลภายนอกดังกล่าว เพื่อกำหนดเงื่อนไขข้อกำหนดสิทธิและหน้าที่ในการประมวลผลข้อมูลส่วนบุคคลระหว่างคู่สัญญา และรับประกัน ความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลดังกล่าว

ข้อ 8 การกำหนดระยะเวลาการรักษาข้อมูล (Data Retention Guideline)

8.1. บริษัทได้กำหนดกรอบการพิจารณาระยะเวลาในการเก็บรักษาข้อมูลส่วนบุคคล (Data Retention Guideline) โดย พิจารณาตามหลักการความจำเป็นเป็นสำคัญภายใต้กรอบการพิจารณาความจำเป็น ดังนี้

- หากมีระยะเวลาตามกฎหมาย ระบุชัดเจนให้เก็บรักษาข้อมูลส่วนบุคคลส่วนใดไว้เป็นระยะเวลานานเท่าใด บริษัทกำหนดให้มีการจัดเก็บตามกำหนดเวลานั้น และในกรณีการเก็บรักษาข้อมูลส่วนบุคคลส่วนใดอยู่ภายใต้เกณฑ์การเก็บรักษาของกฎหมายที่แตกต่างกัน บริษัทกำหนดกรอบการเก็บรักษาข้อมูลส่วนบุคคลไว้เป็นระยะเวลาตามกรอบเวลาสูงสุดที่กฎหมายทั้งหมดกำหนดไว้
- กรณีเป็นการเก็บข้อมูลส่วนบุคคล เนื่องจากความจำเป็นที่พิจารณาโดยอาศัยความสัมพันธ์ต่างๆ ที่บริษัทมีกับเจ้าของข้อมูล เช่น ด้วยฐานสัญญาให้เก็บข้อมูลไว้เท่าที่จำเป็นเพื่อการปฏิบัติตามหน้าที่ในสัญญา กำหนดระยะเวลา ในการเก็บรักษาข้อมูลดังกล่าวตลอดระยะเวลาการให้บริการ หรือตราบเท่าที่จะมีการยกเลิกสัญญาหรือความสัมพันธ์ที่เกี่ยวข้อง ซึ่งอาจมีระยะเวลาแน่นอนหรือไม่ก็เป็นได้ แต่ต้องมีการกำหนดกรอบระยะเวลาการเก็บรักษาที่ชัดเจนแน่นอนซึ่งคาดหมายได้โดยเจ้าของข้อมูล
- กรณีเป็นการเก็บข้อมูลเพื่อประโยชน์อันชอบธรรม ได้ดำเนินการเก็บข้อมูลดังกล่าวไว้ตามกรอบที่เหมาะสมเพื่อการใช้สิทธิในแต่ละกรณีดังกล่าว เช่น ตามระยะเวลาอายุความ กรณีการฟ้องร้องต่อสู้สิทธิต่างๆ ทั้งนี้ หลักการสำคัญที่ได้พิจารณาคือ การประมวลผลข้อมูลส่วนบุคคลดังกล่าวต้องไม่กระทบสิทธิของเจ้าของข้อมูลมากเกินสมควร และบริษัทได้กำหนดให้สิทธิเจ้าของข้อมูลในการคัดค้านการประมวลผลข้อมูลส่วนบุคคลโดยฐานดังกล่าวได้ตามสิทธิที่มี
- กรณีการประมวลผลข้อมูลส่วนบุคคลภายใต้ฐานความยินยอมให้เก็บข้อมูลได้ ตราบเท่าที่เจ้าของข้อมูลยังไม่ได้ใช้สิทธิในการถอนความยินยอม ซึ่งเป็นสิทธิอิสระที่เจ้าของข้อมูลสามารถดำเนินการได้ ตลอดระยะเวลาตามสิทธิที่ตนเองมี และบริษัทเคารพสิทธิในการตัดสินใจดังกล่าว
- กรณีข้อมูลส่วนบุคคลที่บริษัทประมวลผลเป็นข้อมูลส่วนบุคคลอ่อนไหว เช่น ประวัติอาชญากรรม หรือประวัติสุขภาพการรักษาพยาบาล หรือข้อมูลชีวภาพอื่นๆ บริษัทได้ใช้ความระมัดระวังในการบริหารจัดการ และประมวลผลข้อมูลส่วนบุคคลด้วยมาตรฐานที่สูงขึ้น โดยเฉพาะระยะเวลาในการทำลายข้อมูลดังกล่าว และจำกัดเวลาให้มีการลบหรือทำลายในทันทีที่หมดความจำเป็น

8.2. เมื่อพ้นระยะเวลาเก็บรักษาข้อมูลส่วนบุคคลตามกรอบที่กำหนดไว้แล้ว บริษัทจะลบทำลายข้อมูลส่วนบุคคลดังกล่าว หรือดำเนินการทำให้ข้อมูลกลายเป็นข้อมูลนิรนามขึ้นอยู่กับลักษณะของข้อมูล ซึ่งบริษัทกำหนดรอบในการทำลายเอกสารที่ครบกำหนดความจำเป็นเป็นรายปีปฏิทิน ทั้งนี้ สำหรับการทำลายข้อมูลที่อยู่ในรูปแบบกระดาษ บริษัทกำหนดให้ผู้ให้บริการภายนอกเป็นผู้ดำเนินการดังกล่าว โดยงรับประกันการจัดทำข้อตกลงและเงื่อนไขการประมวลผลข้อมูลส่วนบุคคลและได้รับการประกันความสมบูรณ์ในการทำลายเอกสารดังกล่าว นอกจากนี้ สำหรับ ข้อมูลอิเล็กทรอนิกส์ได้ดำเนินการ

ทำลายทางเทคนิคอย่างเหมาะสม และหากมีการบันทึกข้อมูลดังกล่าวในอุปกรณ์หรือเครื่องมืออื่น เช่น USB หรือคอมพิวเตอร์ใดๆ ได้ใช้ความพยายามอย่างที่สุดในการทำลายข้อมูลดังกล่าวทั้งหมด ตามบันทึกรายการการประมวลผลข้อมูลที่มีการจัดเก็บไว้

8.3. สำหรับกระบวนการในการบริหารจัดการเอกสาร บริษัทกำหนดกระบวนการ ดังนี้

- ฝ่ายงานที่รับผิดชอบข้อมูลและเอกสารดังกล่าว มีหน้าที่ในการตรวจสอบเอกสารที่ถึงกำหนดเคลื่อนย้ายหรือทำลายตามนโยบายการเก็บรักษาที่ได้ประกาศไว้
- เมื่อถึงกำหนดระยะเวลาการเคลื่อนย้ายหรือทำลาย ฝ่ายนั้นต้องปิดกล่องผนึกพร้อมลงวันที่ และแจ้งส่งกล่องเอกสารดังกล่าวเพื่อให้ฝ่ายบริหารสำนักงาน ซึ่งจะทำหน้าที่เพียงการบริหารจัดการการเข้า-ออกของเอกสาร
- กรณีการเคลื่อนย้ายเอกสารไปโกดัง หรือการทำลายเอกสารได้กำหนดให้มีตัวแทนของฝ่ายงานที่เกี่ยวข้อง ซึ่งเป็นเจ้าของข้อมูล และฝ่ายบริหารสำนักงานไปร่วมในการดำเนินการดังกล่าว โดยรับผิดชอบจัดทำบันทึกและสารบัญระบบ เอกสารร่วมกัน เพื่อประโยชน์ในการติดตามเอกสารดังกล่าว
- การทำลายเอกสารโดยผู้ให้บริการภายนอก ได้กำหนดให้มีการดำเนินการโดยรับประกันความสมบูรณ์และการรักษาความมั่นคงปลอดภัยของข้อมูล โดยมีการจัดทำสัญญาการประมวลผลข้อมูลส่วนบุคคลระหว่างบริษัทและผู้ให้บริการภายนอก

ข้อ 9 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

9.1. บริษัทกำหนดการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ภายใต้หลักการป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไขหรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ ภายใต้กรอบการรับประกัน ดังนี้

- ข้อมูลทั้งหมดจะได้รับการเก็บรักษาไว้อย่างปลอดภัยและเป็นความลับ (Confidentiality) โดยถือว่าข้อมูลส่วนบุคคลทั้งหมดโดยเฉพาะข้อมูลส่วนบุคคลอ่อนไหวเป็นข้อมูลความลับสูงสุด
- ข้อมูลทั้งหมดต้องเป็นข้อมูลที่ถูกต้องเชื่อถือได้เป็นไปตามข้อมูลที่ทางผู้เป็นเจ้าของข้อมูลได้ให้ข้อมูลดังกล่าวขึ้นมา โดยไม่เกิดการแก้ไขโดยไม่ได้รับอนุญาต (Integrity)
- ข้อมูลต้องมีความพร้อมใช้งานได้ทันทีที่ต้องการ (Availability)

9.2. บริษัทกำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ซึ่งครอบคลุมถึงมาตรการป้องกันด้านการบริหารจัดการผ่านโครงสร้างการจัดตั้งที่กำหนดขึ้น มาตรการป้องกันด้านเทคนิค และมาตรการป้องกันทางกายภาพ ภายใต้หลักการในการควบคุมเงื่อนไขการเข้าถึงและเข้าใช้ข้อมูลส่วนบุคคลในแต่ละระดับข้อมูลผ่านระบบ Authorization Matrix ตาม Role-Based การจัดการระบบ เพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง การเปลี่ยนแปลง การลบ หรือถ่ายโอนข้อมูลส่วนบุคคลได้ โดยเฉพาะอย่างยิ่งกรณีส่วนที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอ่อนไหว

9.3. บริษัทกำหนดให้มีการบันทึกและจัดเก็บหลักฐาน (logs) ของการเข้าถึง เปลี่ยนแปลง ข้อมูลส่วนบุคคลในส่วนต่างๆ โดยกำหนดให้ (1) หัวหน้าฝ่ายหรือหน่วยงานที่เกี่ยวข้องรับผิดชอบทำการสอบทานบันทึก Log ของพนักงานภายใต้กำกับดูแลของฝ่ายหรือหน่วยงานของตนตรวจความผิดปกติของ Log อย่างสม่ำเสมอ และ (2) ให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคลตรวจสอบ Log ดังกล่าวตามลำดับ Line of Defenses ที่เกี่ยวข้อง

9.4. ในการดำเนินการควบคุมและบริหารจัดการการประมวลผลข้อมูลส่วนบุคคลทั้งหมด บริษัทกำหนดให้ทุกหน่วยงานต้องดำเนินการภายใต้กรอบ Maker-Checker และมีการตรวจสอบ ทดสอบประสิทธิภาพในการทำงานของมาตรการและกลไกต่างๆ อย่างสม่ำเสมอ

9.5. กรณีที่บริษัทใช้เครื่องมืออุปกรณ์ หรือทรัพย์สินสารสนเทศในการเก็บและประมวลผลข้อมูลส่วนบุคคลของเจ้าของข้อมูลไม่ว่ากลุ่มใดก็ตาม บริษัทได้ดำเนินการจัดทำทะเบียนทรัพย์สินดังกล่าวให้ครบถ้วน และกำหนดจำกัดสิทธิหรือเงื่อนไขในการใช้ทรัพย์สินสารสนเทศที่เป็นของพนักงานแต่ละคน (BYOD) ไว้อย่างชัดเจน เพื่อให้มีมาตรฐานในการรักษาความมั่นคงของข้อมูลส่วนบุคคลในทุกอุปกรณ์ทรัพย์สินสารสนเทศ ทั้งนี้ได้จำกัดการใช้ BYOD เพื่อการเก็บรักษาหรือประมวลผลข้อมูลส่วนบุคคลให้เหลือน้อยที่สุด เพื่อป้องกันความเสี่ยงของการละเมิดหรือรั่วไหลของข้อมูลส่วนบุคคล

9.6. กำหนดนโยบายการสำรองข้อมูลส่วนบุคลที่มีความสำคัญทั้งหมด ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง เพื่อรับประกันให้ข้อมูลส่วนบุคคลดังกล่าวพร้อมใช้งานได้ตลอดเวลาโดยไม่หยุดชะงัก ทั้งนี้ ได้จัดให้มีการทดสอบข้อมูลสำรอง และกระบวนการกู้คืนข้อมูล (Data Recovery) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูลส่วนบุคคลทั้งหมด ที่มีการประมวลผลมีความถูกต้องครบถ้วนและสามารถใช้งานได้ภายในระยะเวลาที่กำหนด ทั้งนี้ สำหรับการใช้ Data Recovery Site บริษัทจะพิจารณาใช้บริการผู้ให้บริการภายในประเทศไทยเป็นหลักก่อน เพื่อรับประกันความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

9.7. บริษัทกำหนดกระบวนการในการควบคุม และรักษาความปลอดภัยของการประมวลผลข้อมูลส่วนบุคคล โดยผู้ให้บริการภายนอกอย่างชัดเจน และได้กำหนดมาตรฐานตั้งแต่กระบวนการคัดเลือกผู้ให้บริการภายนอก การจัดทำสัญญา การกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ที่ผู้ให้บริการภายนอกอาจเข้าถึง โดยจำกัดการเข้าถึงและการใช้งานเฉพาะเท่าที่จำเป็นเท่านั้น และรับประกันการรักษามาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่ผู้ให้บริการดังกล่าวอาจเข้าถึงให้ได้มาตรฐานเดียวกันกับมาตรฐานของบริษัท ทั้งนี้ได้กำหนดให้มีหน่วยงานเพื่อทำหน้าที่ในการติดตามและตรวจสอบการปฏิบัติหน้าที่ของผู้ให้บริการภายนอกให้เป็นไปตามมาตรฐานที่กำหนดตามกำหนดระยะเวลาเป็นปกติ โดยหากพบความผิดปกติ หรือการละเมิดให้ดำเนินการลงโทษผู้ให้บริการ ดังกล่าวทันที โดยรับประกันไม่ให้เกิดผลกระทบต่อความต่อเนื่องในการให้บริการของบริษัท

9.8. บริษัทกำหนดให้มีการทบทวนนโยบายและมาตรการจัดการและจัดเก็บข้อมูลเพื่อรักษาความมั่นคงปลอดภัยดังกล่าวเป็นประจำอย่างน้อยปีละ 1 ครั้ง

ข้อ 10 การบริหารจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

10.1. บริษัทกำหนดให้คณะทำงานคุ้มครองข้อมูลส่วนบุคคล มีหน้าที่ในการกำหนดนโยบายและมาตรการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล หรือเกิดเป็นเหตุละเมิดข้อมูลส่วนบุคคล โดยประสานกับหน่วยงานที่เกี่ยวข้อง ทั้งนี้ คณะทำงานคุ้มครองข้อมูลส่วนบุคคลเป็นผู้ทำหน้าที่รับแจ้งและบริหารจัดการเหตุการณ์ดังกล่าวก่อน และกำหนดให้มีการทบทวนแผนการดำเนินการดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงที่ส่งผลกระทบกับแผนดังกล่าว

10.2. กรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคล คณะทำงานคุ้มครองข้อมูลส่วนบุคคล ทำหน้าที่ในการรายงานเหตุการณ์ดังกล่าว ให้คณะกรรมการบริษัท ทราบเพื่อจัดเตรียมเอกสารรายงานจัดส่ง ให้แก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ภายในกรอบระยะเวลาการรายงาน 72 ชั่วโมงนับแต่ทราบเหตุ และให้แจ้งเหตุแก่เจ้าของข้อมูลส่วนบุคคล กรณีได้รับผลกระทบ

10.3. ภายหลังสิ้นสุดเหตุละเมิดดังกล่าว คณะทำงานคุ้มครองข้อมูลส่วนบุคคลมีหน้าที่ในการตรวจสอบ และสอบทานเพื่อพิจารณา Root Cause ของเหตุการณ์ดังกล่าวเพื่อจัดทำรายงานเสนอต่อคณะกรรมการบริษัททราบ และเพื่อเป็นแผนการในการปรับปรุงแก้ไขป้องกันเหตุละเมิดที่อาจเกิดขึ้นในอนาคตต่อไป

ข้อ 11 การทบทวนหรือปรับปรุงนโยบาย

บริษัทกำหนดให้มีการทบทวนหรือปรับปรุงนโยบายฉบับนี้ โดย ประธานกรรมการบริหารและกรรมการผู้จัดการ ด้วยการพิจารณาจากรายงานการปฏิบัติตามนโยบายการบริหารจัดการคุ้มครองการประมวลผลข้อมูลที่นำเสนอ โดยคณะกรรมการตรวจสอบอย่างน้อยปีละ 1 ครั้งหรือกรณีที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญต่อธุรกิจบริษัท หรือกระบวนการประมวลผลข้อมูลส่วนบุคคลที่บริษัทดำเนินการเพื่อให้นโยบายเป็นปัจจุบันอยู่เสมอ โดยจะมีการเสนอให้คณะกรรมการบริษัทพิจารณารับรองทุกครั้งที่มีการทบทวนและแก้ไขเปลี่ยนแปลง