มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล

บริษัท ศรีนานาพร มาร์เก็ตติ้ง จำกัด (มหาชน)

1) **หลักการและเหตุผล**

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล พ.ศ. 2563 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 (“กฎหมาย”) กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลจะต้องดำเนินการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล

วัตถุประสงค์ของการรักษาความปลอดภัยเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลและอำนาจในการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งกฎหมายรับรองไว้ให้ ด้วยเหตุนี้ การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นหน้าที่ประการหนึ่งตามกฎหมาย ที่กำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคล (รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคล) จะต้องปฏิบัติเพื่อป้องกันมิให้เกิดสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งจะทำให้เกิดการละเมิดข้อมูลส่วนบุคคล

2) **การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล**

บริษัทจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลโดยครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามกฎหมาย ทั้งมาตรการป้องกันด้านการบริหารจัดการ มาตรการป้องกันด้านเทคนิค และมาตรการป้องกันทางกายภาพ โดยดำเนินการดังนี้

2.1) มาตรการป้องกันด้านการบริหารจัดการ

2.1.1) แจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามนโยบายนี้ ให้แก่คณะกรรมการ กรรมการ ผู้บริหาร พนักงานหรือผู้ปฏิบัติงานทุกระดับ และลูกจ้างทุกประเภทของบริษัท ตลอดจนคู่ค้า พันธมิตรทางธุรกิจ และ/หรือผู้มีส่วนได้เสียของบริษัททราบ รวมถึงสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าวปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด

2.1.2) ระบุความเสี่ยงที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศ การป้องกันความเสี่ยงที่อาจเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล โดยเป็นไปตามนโยบายการรักษาความปลอดภัยทางสารสนเทศ กำหนดหน้าที่รับผิดชอบให้แก่ตัวแทนบริษัทในการดำเนินการเมื่อเกิดเหตุละเมิด และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล ดังนี้

2.1.2.1) กำหนดตัวพนักงานผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่ตัวแทนของบริษัทให้ชัดเจน เช่น การส่งอีเมล และแจ้งทางโทรศัพท์กรณีเป็นเหตุละเมิดที่มีความรุนแรงและเร่งด่วน

2.1.2.2) กำหนดวิธีปฏิบัติให้ตัวแทนของบริษัทต้องดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลได้ภายใน 72 ชั่วโมง นับแต่ทราบเหตุ

2.1.2.3) การแจ้งเหตุละเมิดตามข้อ 2.1.2.2) อาจได้รับยกเว้นไม่ต้องดำเนินการก็ได้ หากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ทั้งนี้ เมื่อมีเหตุการละเมิดข้อมูลส่วนบุคคล บริษัทต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยทุกครั้ง

2.1.3) กำหนดเกี่ยวกับการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (User Responsibilities) แบ่งเป็นรูปแบบต่างๆ เช่น สิทธิในการเข้าดู แก้ไข เพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบทำลาย

2.1.4) บริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

2.1.5) จัดให้มีวิธีการเพื่อตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

2.1.6) ในกรณีที่มีการฝ่าฝืนไม่ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยนี้เนื่องจากความบกพร่องของบริษัทและทำให้เกิดการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคล บริษัทจะแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดของเหตุการณ์และแผนเยียวยาความเสียหายจากการละเมิดหรือรั่วไหลดังกล่าวโดยเร็ว อย่างไรก็ตาม บริษัทจะไม่รับผิดชอบในความเสียหายใดๆ อันเกิดจากการใช้ การเปิดเผย รวมถึงการประมาทเลินเล่อของเจ้าของข้อมูลหรือบุคคลอื่นที่ได้รับความยินยอมจากเจ้าของข้อมูล

2.1.7) เมื่อพ้นระยะเวลาการใช้งานข้อมูลส่วนบุคคลหรือไม่มีความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลอีกต่อไป บริษัทจะลบหรือทำลายข้อมูลส่วนบุคคลออกจากระบบการจัดเก็บ เว้นแต่ในกรณีที่ต้องเก็บรักษาข้อมูลส่วนบุคคลไว้ตามที่กฎหมายกำหนด

2.1.8) บริษัทมีการดำเนินการสอบทานและประเมินประสิทธิภาพของระบบรักษาข้อมูลส่วนบุคคลโดยหน่วยงานตรวจสอบภายใน

2.2) มาตรการป้องกันด้านเทคนิค

2.2.1) จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

2.2.2) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการจัดการข้อมูล ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย ซึ่งรวมถึงแต่ไม่จำกัดเพียง

2.2.2.1) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและส่วนประกอบของระบบสารสนเทศที่สำคัญที่มีการพิสูจน์และยืนยันตัวตน และการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงและใช้งานที่เหมาะสม โดยคำนึงถึงหลักการให้สิทธิเท่าที่จำเป็น ตามหลักการให้สิทธิที่น้อยที่สุดเท่าที่จำเป็น

2.2.2.2) การบริหารจัดการการเข้าถึงของผู้ใช้งานที่เหมาะสม ซึ่งอาจรวมถึงการลงทะเบียนและการถอนสิทธิผู้ใช้งาน การจัดการสิทธิการเข้าถึงของผู้ใช้งาน การบริหารจัดการสิทธิการเข้าถึงตามสิทธิ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน และการถอดถอนหรือปรับปรุงสิทธิการเข้าถึง

2.2.3) การจัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง ทั้งนี้เป็นไปตามหลักเกณฑ์และวิธีปฏิบัติทางสารสนเทศของบริษัท

2.3) มาตรการป้องกันทางกายภาพ

2.3.1) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง และมีการล็อคตู้เก็บเอกสารข้อมูลส่วนบุคคล เป็นต้น ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

2.3.2) การกำหนดผู้ที่ได้รับอนุญาตให้เข้าถึงอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล ตามหน้าที่ความรับผิดชอบ เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลส่วนบุคคล การลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล การลักลอบนำอุปกรณ์เข้าออก การดำเนินการการป้องกันและระมัดระวังไม่ให้ข้อมูลรั่วไหลหรือถูกละเมิดอย่างหนึ่งอย่างใด เช่น ไม่เปิดไฟล์ข้อมูลส่วนบุคคลในที่สาธารณะ ปิด/เก็บข้อมูลส่วนบุคคลให้มิดชิดเมื่อลุกออกจากโต๊ะ กรณีการใช้เครื่องพิมพ์เอกสารร่วมกันต้องลบไฟล์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลออกจากหน้า screen เครื่องพิมพ์ทุกครั้งและออกจากระบบ (Log out) ให้เรียบร้อย จัดทำบันทึกคำร้องขอเข้าถึงข้อมูลส่วนบุคคลและทำลายเอกสารข้อมูลส่วนบุคคลด้วยตนเองทุกครั้งโดยไม่ฝากบุคคลอื่นทำลายแทน เป็นต้น

2.4) ข้อตกลงระหว่างบริษัทและผู้ประมวลผลข้อมูลส่วนบุคคล

กรณีมีข้อตกลงระหว่างบริษัทและผู้ประมวลผลข้อมูลส่วนบุคคล บริษัทจะกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเทียบเท่าหรือดีกว่ามาตรการตามนโยบายนี้ เพื่อป้องกันการสูญหาย การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ หรือกระทำโดยปราศจากอำนาจโดยชอบด้วยกฎหมาย รวมทั้งแจ้งให้บริษัททราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น ทั้งนี้ความเข้มข้นของมาตรการ ให้เป็นไปตามระดับความเสี่ยง หรือ ความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย โดยมิชอบ

2.5) การส่ง การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

การส่ง การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ รวมถึงการนำข้อมูลส่วนบุคคลไปเก็บบนฐานข้อมูลในระบบอื่นใด ซึ่งผู้ให้บริการรับโอนข้อมูลหรือบริการเก็บรักษาข้อมูลอยู่ต่างประเทศ ประเทศปลายทางที่เก็บรักษาข้อมูลต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เทียบเท่าหรือดีกว่ามาตรการตามนโยบายนี้

2.6) การฝ่าฝืนมาตรการการรักษาความมั่นคงปลอดภัยของบริษัท

ในกรณีที่มีการฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัยของบริษัท จนเป็นเหตุให้มีการละเมิดข้อมูลส่วนบุคคล หรือข้อมูลส่วนบุคคลรั่วไหลสู่สาธารณะ บริษัทจะดำเนินการแจ้งเจ้าของข้อมูลให้ทราบโดยเร็ว รวมทั้งแจ้งแผนการเยียวยาความเสียหายจากการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคลสู่สาธารณะในกรณีที่เกิดจากความบกพร่องของบริษัท

3) **การทบทวนมาตรการ**

บริษัทต้องจัดให้มีการทบทวนมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลฉบับนี้เป็นประจำทุกปี เมื่อมีความจำเป็น และ/หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป

4) **คำสงวนสิทธิ**

บริษัทจะไม่รับผิดชอบกรณีที่ความเสียหายใดๆ อันเกิดจากการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่สาม รวมถึงการละเลยหรือเพิกเฉย การออกจากระบบ (Log Out) ฐานข้อมูลหรือระบบสื่อสารสังคมออนไลน์ของบริษัท โดยการกระทำของเจ้าของข้อมูลหรือบุคคลอื่นซึ่งได้รับความยินยอมจากเจ้าของข้อมูล

มาตรการรักษาความมั่นคงปลอดภัยฉบับนี้มีผลตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2565 เป็นต้นไป

บริษัท ศรีนานาพร มาร์เก็ตติ้ง จำกัด (มหาชน)