บริษัท พอช เมดิก้า ไลฟ์เทค จำกัด (มหาชน) (สำนักงานใหญ่)
27/8 ซอย 01 กาญจนาภิเษก 11/1 แขวงคันนายาว เขตคันนายาว กรุงเทพมหานคร 10230
โทรศัพท์ +66 (0) 2097-7700
เลขประจำตัวผู้เสียภาษี: 0107568000094

มาตรการรักษาความมั่นคงปลอดภัย

และการป้องกันและบรรเทาการรั่วไหลของข้อมูลส่วนบุคคล

กลุ่มบริษัท พอช เมดิก้า ไลฟ์เทค จำกัด (มหาชน) ("กลุ่มบริษัทฯ) ให้ความสำคัญเป็นอย่างยิ่งต่อการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยมาตรการฉบับนี้จัดทำขึ้นเพื่อป้องกันมิให้ข้อมูลส่วนบุคคลถูกเข้าถึง สูญหาย ทำลาย ใช้ ดัดแปลง แก้ไข หรือเปิดเผยโดยไม่ได้รับอนุญาต

1. **คำนิยาม**

"บริษัทฯ" หมายถึง บริษัท พอช เมดิก้า ไลฟ์เทค จำกัด (มหาชน)

"กลุ่มบริษัทฯ" หมายถึง บริษัท พอช เมดิก้า ไลฟ์เทค จำกัด (มหาชน) และบริษัทย่อย

"บริษัทย่อย" หมายถึง บริษัทที่มีลักษณะใดลักษณะหนึ่งดังนี้

(1) บริษัทที่บริษัทฯ มีอำนาจควบคุมกิจการ

(2) บริษัทที่อยู่ภายใต้อำนาจควบคุมกิจการของบริษัทตาม (1) ต่อไปเป็นทอดๆ โดยเริ่มจากการอยู่ภายใต้อำนาจควบคุมกิจการของบริษัทตาม (1)

"ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

"ข้อมูลที่มีความอ่อนไหว" หมายถึง ข้อมูลส่วนบุคคลที่เกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ เช่น การสแกนใบหน้า การสแกนลายนิ้วมือ เป็นต้น หรือข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่กฎหมายประกาศกำหนด

2. **มาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล**

2.1 สร้างความตระหนักรู้ และฝึกอบรมเพื่อเสริมสร้างการดูแลด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลให้แก่พนักงาน โดยการเผยแพร่ข้อมูลข่าวสาร ให้ความรู้ และแนวทางการปฏิบัติตามกฎหมายอย่างเคร่งครัด

2.2 พนักงานของกลุ่มบริษัทฯ ทุกคนต้องปฏิบัติตามแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด โดยหากฝ่าฝืนแนวปฏิบัติแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล จะได้รับการลงโทษตามข้อบังคับเกี่ยวกับการทำงาน และกฎหมายอื่นๆ ที่เกี่ยวข้อง

2.3 จำกัดผู้มีสิทธิ์เข้าถึงข้อมูลส่วนบุคคล (Access Control) เท่าที่จำเป็นต้องใช้ข้อมูลส่วนบุคคลเพื่อการปฏิบัติงาน โดยพนักงานจะต้องรักษาข้อมูลส่วนบุคคลเป็นความลับ

2.4 กำหนดมาตรการที่เข้มงวดและเหมาะสม สำหรับการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data) หรือข้อมูลที่อาจกระทบต่อความรู้สึก ความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน

2.5 ฝ่าย/แผนกที่ปฏิบัติหน้าที่เกี่ยวกับข้อมูลส่วนบุคคลต้องจัดทำบันทึกรายงานกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing Activities: RoPA) โดยระบุพนักงานภายในฝ่าย/แผนกที่สามารถเข้าถึงข้อมูลส่วนบุคคล และกำหนดผู้มีอำนาจอนุญาตกรณีมีผู้ขอข้อมูลส่วนบุคคล

2.6 กรณีที่กลุ่มบริษัทฯ ว่าจ้างผู้รับจ้างทำหน้าที่เกี่ยวข้องกับข้อมูลส่วนบุคคล กลุ่มบริษัทฯ จะคัดเลือกผู้รับจ้างที่มีมาตรการในการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสมและกำหนดให้ผู้รับจ้างลงนามในข้อตกลงระหว่างผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) และจัดเตรียมข้อมูลส่วนบุคคลเพียงเท่าที่จำเป็นต่อวัตถุประสงค์ของการว่าจ้างเท่านั้น

2.7 กลุ่มบริษัทฯ กำหนดให้พนักงานทุกคนปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยของสารสนเทศโดยเคร่งครัด และหากพนักงานผู้ใดฝ่าฝืนจะได้รับการลงโทษตามข้อบังคับเกี่ยวกับการทำงาน และกฎหมายอื่นๆ ที่เกี่ยวข้อง

3. การป้องกันและบรรเทาการรั่วไหลของข้อมูลส่วนบุคคล

3.1 แต่งตั้งคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) โดยเป็นตัวแทนจากฝ่าย/แผนกที่ปฏิบัติหน้าที่เกี่ยวกับข้อมูลส่วนบุคคล ทำหน้าที่ดังต่อไปนี้

3.1.1 ให้คำแนะนำพนักงาน ผู้รับจ้าง และผู้ประมวลผลข้อมูลข้อมูลส่วนบุคคลเกี่ยวกับการปฏิบัติหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

3.1.2 ตรวจสอบการดำเนินงานของพนักงาน ผู้รับจ้าง และผู้ประมวลผลข้อมูลส่วนบุคคลเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

3.1.3 ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3.1.4 รักษาความลับของข้อมูลส่วนบุคคลที่ตนล่วงรู้หรือได้มาเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562

3.2 กรณีเกิดการรั่วไหลของข้อมูลส่วนบุคคล กลุ่มบริษัทฯ กำหนดแนวทางการดำเนินการดังนี้

3.2.1 พนักงานที่ทราบเรื่องจะต้องแจ้งยังเลขานุการคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลโดยทันที

3.2.2 เลขานุการคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทำการตรวจสอบในเบื้องต้นถึงสาเหตุที่มาและระบุจุดต้นเหตุของการรั่วไหล

3.2.3 เลขานุการคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเรียกประชุมคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

3.2.4 ที่ประชุมคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลร่วมกันประเมินความเสี่ยง โดยพิจารณาผลกระทบต่อสิทธิและเสรีภาพขั้นพื้นฐาน ผลกระทบต่อชีวิตและทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล

(1) กรณีคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีความเห็นว่า ไม่มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมีผลกระทบต่อชีวิตและทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล เลขานุการคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทำการจดบันทึกข้อมูลการรั่วไหลของข้อมูลส่วนบุคคล โดยไม่ต้องแจ้งต่อเจ้าของข้อมูลส่วนบุคคลและสำนักงานคุ้มครองข้อมูลส่วนบุคคล

(2) กรณีคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีความเห็นว่า มีผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล หรือมีผลกระทบต่อชีวิตและทรัพย์สินของเจ้าของข้อมูลส่วนบุคคล คณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลกำหนดมาตรการการเยียวยาที่สอดคล้องกับความเสียหายที่เจ้าของข้อมูลส่วนบุคคลได้รับ

และแจ้งต่อเจ้าของข้อมูลส่วนบุคคลและสำนักงานคุ้มครองข้อมูลส่วนบุคคล ภายใน 72 ชั่วโมง และเลขานุการคณะทำงานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทำการจดบันทึกข้อมูลการรั่วไหลของข้อมูลส่วนบุคคล

3.3 นำเหตุการณ์การรั่วไหลของข้อมูลส่วนบุคคลมาวิเคราะห์ ทบทวนกระบวนการทำงาน และกำหนดมาตรการใหม่หรือแก้ไขปรับปรุงมาตรการเดิมให้มีความเหมาะสมเพื่อป้องกันการเกิดเหตุการณ์ซ้ำ และพิจารณาการลงโทษตามข้อบังคับเกี่ยวกับการทำงานและ/หรือดำเนินการทางกฎหมายกับผู้กระทำความผิด

4. การทบทวนมาตรการ

กลุ่มบริษัทฯ จะทบทวนมาตรการฉบับนี้เมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้เกิดประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

ประกาศ ณ วันที่ 12 เดือนพฤศจิกายน พ.ศ. 2568

(แพทย์หญิง วิวรรณ เดชสุนทรวัฒน์)
ประธานเจ้าหน้าที่บริหาร
กลุ่มบริษัท พอช เมดิก้า ไลฟ์เทค จำกัด (มหาชน)