

ระเบียบปฏิบัติเกี่ยวกับการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคล ของบริษัท แม่น้ำสแตนเลสไวร์ จำกัด (มหาชน)

ด้วยบริษัท แม่น้ำสแตนเลสไวร์ จำกัด (มหาชน) ตระหนักถึงความสำคัญของข้อมูลส่วนบุคคลและข้อมูลอื่น อีกทั้งเพื่อให้การดำเนินงานของบริษัท แม่น้ำสแตนเลสไวร์ จำกัด (มหาชน) มีความโปร่งใสและความรับผิดชอบในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลของท่านตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงกฎหมายอื่นที่เกี่ยวข้อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล จึงออกระเบียบนี้เพื่อเป็นแนวทางในการทำงานต่อไปดังนี้

ข้อ ๑ ระเบียบนี้เรียกว่า ระเบียบปฏิบัติเกี่ยวกับการปฏิบัติงานเกี่ยวกับข้อมูลส่วนบุคคลของบริษัท แม่น้ำสแตนเลสไวร์ จำกัด (มหาชน)

ข้อ ๒ ระเบียบนี้ให้มีผลใช้บังคับตั้งแต่วันที่ ๑ มิถุนายน ๒๕๖๕ เป็นต้นไป

ข้อ ๓ การรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลที่ระเบียบนี้ไม่ได้กำหนดเอาไว้ ให้ดำเนินการไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ รวมถึงกฎหมายลำดับรอง และนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัท แม่น้ำสแตนเลสไวร์ จำกัด (มหาชน)

ข้อ ๔ นิยามศัพท์

“บริษัท” หมายถึง บริษัท แม่น้ำสแตนเลสไวร์ จำกัด (มหาชน)

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม และข้อมูลของนิติบุคคล

“เจ้าของข้อมูลส่วนบุคคล” หมายความว่า บุคคลซึ่งข้อมูลนั้นระบุตัวตนไปถึงได้ ไม่ว่าจะ เป็นข้อมูลทางตรง ข้อมูลทางอ้อม ข้อมูลอ่อนไหว

“การประมวลผลข้อมูลส่วนบุคคล” หมายถึง การดำเนินการใด ๆ กับข้อมูลส่วนบุคคลไม่ว่าจะเป็นการเก็บรวบรวม บันทึก สำเนา จัดระเบียบ เก็บรักษา ปรับปรุง เปลี่ยนแปลง ใช้ กู้คืน เผยแพร่ ส่งต่อ เผยแพร่ โอน รวม ลบ ทำลาย

“ผู้ควบคุมข้อมูลส่วนบุคคล” หมายความว่า บริษัท แม่น้ำสแตนเลสไวร์ จำกัด (มหาชน) ในฐานะผู้มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

“ผู้ประมวลผลข้อมูลส่วนบุคคล” หมายถึง บุคคลธรรมดา หรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่ง หรือกระทำในนามของผู้ควบคุมข้อมูลส่วนบุคคล

“เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล” หมายความว่า บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของบริษัท แม่น้ำสแตนเลสไวร์ จำกัด (มหาชน) ในฐานะผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล

“ผู้บริหาร” หมายถึง ผู้บริหารในแผนก หรือฝ่าย หรือสาขาที่มีอำนาจบังคับบัญชาสูงสุดในแผนก หรือฝ่าย หรือสาขานั้น ซึ่งบริษัทกำหนดให้เป็นผู้มีหน้าที่ควบคุมกำกับให้การรวบรวม ใช้ เปิดเผย รวมถึง มาตรการรักษาความมั่นคงปลอดภัย ในแผนหรือฝ่ายหรือสาขานั้นให้เป็นไปตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และระเบียบนี้ ซึ่งบริษัทจะประกาศรายชื่อเอาไว้ให้ทราบในระเบียบนี้

“พนักงาน” หมายถึง พนักงานซึ่งผูกพันกับบริษัท แม่น้ำสแตนเลสไวร์ จำกัด (มหาชน) ตามสัญญาจ้างแรงงาน และ/หรือมีนิติสัมพันธ์กันตามกฎหมายคุ้มครองแรงงานในฐานะนายจ้าง ลูกจ้าง

“ข้อมูลอ่อนไหว” หมายความว่า ข้อมูลที่อาจนำไปสู่การเลือกปฏิบัติอัน ได้แก่ เชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ ข้อมูลอื่นที่คณะกรรมการ อาจประกาศออกมาเพิ่มเติม

หมวดที่ ๑ หน้าที่และความรับผิดชอบ

ข้อ ๕ ให้คณะกรรมการบริษัทมีอำนาจ หน้าที่ ดังนี้

- (๑) กำหนดนโยบาย และแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล
- (๒) กำกับดูแลให้มีการดำเนินการตามกฎหมาย นโยบาย และระเบียบที่เกี่ยวข้อง

ข้อ ๖ ผู้บริหารซึ่งมีตำแหน่งดังต่อไปนี้ เป็นผู้กำกับการให้เป็นไปตามกฎหมายและระเบียบในแผนกหรือฝ่ายที่ตนเองมีหน้าที่รับผิดชอบ คือ

- (๑) ผู้จัดการฝ่าย
- (๒) ผู้ช่วยผู้จัดการฝ่าย
- (๓) หัวหน้าแผนก
- (๔) หัวหน้างาน
- (๕) หัวหน้ากะ
- (๖) เจ้าหน้าที่ที่ได้รับมอบหมาย

อนึ่ง รายชื่อผู้บริหาร บริษัทจะออกประกาศให้ทราบ

มีอำนาจและหน้าที่ดังนี้

- (๑) ดำเนินการให้เป็นไปตามข้อกำหนดในการรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลให้เหมาะสมกับลักษณะหรือสภาพของงาน
- (๒) จัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลทั้งทางด้านบริหาร ด้านกายภาพ และด้านเทคนิคสำหรับข้อมูลส่วนบุคคลที่อยู่ในความรับผิดชอบของตน เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น
- (๓) บริหารจัดการให้พนักงานที่อยู่ภายใต้การบังคับบัญชาดำเนินการ ปฏิบัติตามกฎหมาย โดยห้ามไม่ให้รวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย
- (๔) พิจารณาโทษทางวินัยแก่พนักงานที่อยู่ภายใต้บังคับบัญชา ที่ฝ่าฝืนไม่ปฏิบัติตามระเบียบนี้ หรือระเบียบอื่น หรือคำสั่งที่เกี่ยวข้อง หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- (๕) การติดต่อบุคคลภายนอกเพื่อทำการประมวลผลจะต้องมีการทำสัญญากำกับไม่ให้ใช้หรือเปิดเผยข้อมูลโดยไม่ชอบด้วยกฎหมาย รวมถึงควรคัดเลือกบุคคลที่มีนโยบายการคุ้มครองข้อมูลส่วนบุคคล และมีระบบการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

(๖) ดำเนินการและควบคุมการลบหรือทำลายข้อมูลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวม หรือตามที่เจ้าของข้อมูลส่วนบุคคลได้ร้องขอ

(๗) ตรวจสอบ และควบคุม ปรับปรุงข้อมูลส่วนบุคคลให้มีความถูกต้อง ทันสมัยและเป็นปัจจุบัน

(๘) เมื่อพบการรั่วไหล หรือการละเมิดข้อมูลส่วนบุคคลต้องแจ้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลในทันที

(๙) ดำเนินการควบคุมการบันทึกข้อมูลและรายงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่รับผิดชอบ

(๑๐) ประเมินความเสี่ยงที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่ตนรับผิดชอบ บริหารจัดการ และดำเนินการตาม มาตรการที่กำหนดเพื่อลดความเสี่ยง

(๑๑) สร้างความตระหนักรู้เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่พนักงานที่อยู่ภายใต้การบังคับบัญชา

(๑๒) ควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์การจัดเก็บและการประมวลผลข้อมูลส่วนบุคคล

(๑๓) ดำรงไว้ซึ่งความลับของข้อมูลส่วนบุคคล

(๑๔) อนุญาต หรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

ข้อ ๗ ให้แต่งตั้งคณะบุคคลอย่างน้อยต้องประกอบไปด้วยฝ่ายทรัพยากรบุคคล ฝ่ายเทคโนโลยีสารสนเทศ ฝ่ายขายและการตลาด ฝ่ายบัญชีและการเงิน เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัท

ข้อ ๘ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลมีอำนาจหน้าที่ ดังนี้

(๑) ให้ข้อเสนอแนะแก่บริษัท และพนักงานในการรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล และการรักษาความมั่นคงปลอดภัยทั้งทางด้านบริหาร ด้านกายภาพ และด้านเทคนิค

(๒) ทวนสอบ ตรวจสอบการดำเนินงานภายในบริษัท เพื่อให้การรวบรวม ใช้เปิดเผยประมวลผล และการรักษาความมั่นคงปลอดภัยทั้งทางด้านบริหาร ด้านกายภาพ และด้านเทคนิคเป็นไปตามกฎหมาย รวมถึงการตรวจสอบการบันทึกการกิจกรรมข้อมูลส่วนบุคคล (Ropa) และ Privacy Notice ในทุก ๆ ๓ เดือนเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

(๓) ประสานงาน ให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

(๔) รับข้อร้องเรียน ตรวจสอบการกระทำที่ได้รับการร้องเรียน ดำเนินการแก้ไขตามข้อร้องเรียน โกล่เกลี่ยข้อพิพาท พิจารณาความเสียหายและเสนอแนะต่อบริษัท

(๕) ชักซ้อมกรณีข้อมูลรั่วไหล จัดให้มีการตระหนักรู้แก่พนักงาน รวมถึงจัดทำแผนงานประจำปีด้านการคุ้มครองข้อมูลส่วนบุคคล

(๖) ปฏิบัติการอื่นใดตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎหมายอื่นกำหนด

(๗) รักษาความลับที่เกี่ยวข้องกับข้อมูลส่วนบุคคลอันเนื่องมาจากการที่ตนได้ล่วงรู้อันเนื่องมาจากการปฏิบัติหน้าที่

หมวดที่ ๒

การรวบรวม ใช้ เปิดเผยข้อมูลส่วนบุคคล

ข้อ ๙ การรวบรวมข้อมูลส่วนบุคคล ให้พนักงานดำเนินการให้ดำเนินการดังนี้

(๑) ห้ามมิให้รวบรวม โดยไม่ได้รับความยินยอม หรือมีฐานรองรับเพื่อให้เกิดความชอบด้วยกฎหมาย

(๒) การรวบรวมข้อมูลส่วนบุคคลต้องทำโดยชัดแจ้ง เป็นหนังสือ หรือสื่ออิเล็กทรอนิกส์ โดยต้องแยกความยินยอมนั้นออกจากข้อความอื่นอย่างชัดแจ้ง มีแบบ หรือข้อความที่เข้าถึงได้ง่ายและเข้าใจได้ ใช้ภาษาที่เข้าใจง่าย ไม่หลอกลวงหรือทำให้เข้าใจผิดในวัตถุประสงค์

(๓) ในการขอความยินยอมจากเจ้าของข้อมูลส่วนบุคคล ต้องดำเนินการโดยให้เจ้าของข้อมูลเป็นอิสระ

(๔) ให้ดำเนินการตรวจสอบสิทธิ อำนาจและฐานอื่น ๆ เพื่อร้องขอการรวบรวมข้อมูลส่วนบุคคล

(๕) ต้องมีการแจ้งวัตถุประสงค์ในขณะขอความยินยอมเพื่อรวบรวมข้อมูลส่วนบุคคล ก่อนหรือขณะรวบรวมข้อมูลส่วนบุคคล

(๖) ต้องมีการดำเนินการอย่างโปร่งใสโดยการแจ้งรายละเอียดความเป็นส่วนตัว หรือ Privacy Notice ทุกครั้ง

(๗) ห้ามมิให้หลอกลวง เงื่อนไขด้านราคา เงื่อนไขด้านส่วนลด หรือเอาผลเชิงลบอื่น มาเป็นเงื่อนไขในการรวบรวมข้อมูลส่วนบุคคล

(๘) การเก็บรวบรวมข้อมูลส่วนบุคคลต้องดำเนินการโดยน้อยที่สุด เฉพาะที่จำเป็นเท่านั้น โดยต้องดำเนินการสอบถามวัตถุประสงค์ในการนำข้อมูลไปใช้งานเพื่อให้สามารถประเมินว่าควรสำเนาข้อมูลให้ในระดับรายละเอียดเท่าใด เช่น กรณีส่งสินค้าจำเป็นต้องทราบที่อยู่ และ GPS แต่ไม่จำเป็นต้องทราบ วัน เดือน ปีเกิด หรือหมู่โลหิต หรือรหัสไปรษณีย์ เป็นต้น

(๙) ห้ามมิให้รวบรวมข้อมูลอ่อนไหวโดยไม่จำเป็น

ข้อ ๑๐ ห้ามมิให้พนักงานรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ใช่เจ้าของข้อมูลโดยตรง เว้นแต่ในกรณีดังต่อไปนี้

(๑) ได้แจ้งถึงการเก็บรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นให้เจ้าของข้อมูลส่วนบุคคลทราบภายใน ๑๕ วันนับแต่วันที่รวบรวมข้อมูลส่วนบุคคล และได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล

(๒) เป็นการรวบรวมข้อมูลส่วนบุคคลจากแหล่งอื่นที่ไม่ได้รับความยินยอม แต่มีฐานอื่นที่ไม่ต้องขอความยินยอมรองรับ ได้แก่

(ก) ฐานที่ไม่ต้องได้รับความยินยอมกรณีข้อมูลทั่วไป

- ฐานจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะหรือที่เกี่ยวกับการศึกษาวิจัยหรือสถิติซึ่งได้จัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล

- ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล

- ฐานจำเป็นเพื่อการปฏิบัติตามสัญญาซึ่งเจ้าของข้อมูลส่วนบุคคลเป็นคู่สัญญาหรือเพื่อใช้ในการดำเนินการตามคำขอของเจ้าของข้อมูลส่วนบุคคลก่อนเข้าทำสัญญานั้น

- ฐานจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินการกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล

- ฐานจำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล หรือของบุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล เว้นแต่ประโยชน์ดังกล่าวมีความสำคัญน้อยกว่าสิทธิขั้นพื้นฐานในข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคล

- ฐานปฏิบัติตามกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล

(ข) ฐานที่ไม่ต้องได้รับความยินยอมกรณีข้อมูลอ่อนไหว

- ฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคลซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้ ไม่ว่าจะด้วยเหตุใดก็ตาม

- ฐานดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรที่มีวัตถุประสงค์เกี่ยวกับการเมือง ศาสนา ปรัชญา หรือสหภาพแรงงานให้แก่สมาชิก ผู้ซึ่งเคยเป็นสมาชิก หรือผู้ซึ่งมีการติดต่ออย่างสม่ำเสมอกับมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไรตามวัตถุประสงค์ดังกล่าวโดยไม่ได้เปิดเผยข้อมูลส่วนบุคคลนั้นออกไปภายนอกมูลนิธิสมาคม หรือองค์กรที่ไม่แสวงหากำไรนั้น

- ฐานข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล

- ฐานจำเป็นเพื่อการก่อตั้งสิทธิเรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิเรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิเรียกร้องตามกฎหมาย

- ฐานเป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ

(ค) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทาง

การแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ในกรณีที่ไม่ใช่ การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือ ผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่าง เจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์

(ง) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจาก โรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาในราชอาณาจักร หรือการควบคุมมาตรฐาน หรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อ ค้ำครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคล ตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

(จ) การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการ เกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิตามกฎหมาย การคุ้มครองผู้ประสบภัยจากรถ หรือการคุ้มครองทาง สังคม ซึ่งการเก็บรวบรวมข้อมูลส่วนบุคคลเป็นสิ่งจำเป็นในการปฏิบัติตามสิทธิหรือหน้าที่ของผู้ควบคุม ข้อมูลส่วนบุคคลหรือเจ้าของข้อมูลส่วนบุคคล โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้น พื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

(ฉ) การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิติ หรือประโยชน์ สาธารณะอื่น ทั้งนี้ ต้องกระทำเพื่อให้บรรลุวัตถุประสงค์ดังกล่าวเพียงเท่าที่จำเป็นเท่านั้น และได้จัดให้มี มาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล ตามที่ คณะกรรมการประกาศกำหนด

(ช) ประโยชน์สาธารณะที่สำคัญ โดยได้จัดให้มีมาตรการที่เหมาะสมเพื่อคุ้มครองสิทธิ ขั้นพื้นฐานและประโยชน์ของเจ้าของข้อมูลส่วนบุคคล

ข้อ ๑๑ ห้ามมิให้พนักงานรวบรวมข้อมูลส่วนบุคคลที่ยังไม่บรรลุนิติภาวะ ซึ่งมีอายุครบ ๒๐ ปี บริบูรณ์ เว้นแต่

(๑) บุคคลที่มีอายุครบ ๑๗ ปีบริบูรณ์ และได้ทำการสมรสตามกฎหมายสามารถ รวบรวมข้อมูลส่วนบุคคลโดยได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลนั้นได้

(๒) ผู้เยาว์ที่มีฐานะดังเช่นบุคคลที่บรรลุนิติภาวะแล้ว ซึ่งผู้แทนโดยชอบธรรมได้ให้ความ ยินยอมในการทำธุรกิจ การค้า ทำสัญญาจ้างแรงงานไว้แล้ว

(๓) ผู้เยาว์ซึ่งมีอายุ ๑๐ ปี แต่ไม่ครบ ๒๐ ปี โดยได้รับความยินยอมจากผู้แทนโดยชอบ ธรรม หรือกิจการอื่นที่ต้องทำเองเฉพาะตัว อันได้แก่ การได้ไปซึ่งสิทธิ หรือหลุดพ้นจากหน้าที่ หรือการที่ ต้องทำเองเฉพาะตัว หรือการนั้นสมควรแก่ฐานะอุป

(๔) ผู้เยาว์ที่มีอายุต่ำกว่า ๑๐ ปี การขอความยินยอมในการรวบรวมข้อมูลส่วนบุคคล จะต้องขอกับผู้ใช้อำนาจปกครอง

ข้อ ๑๒ การใช้ข้อมูลส่วนบุคคล ให้พนักงานดำเนินการดังนี้

- (๑) ห้ามมิให้ใช้ข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมหรือมีฐานรับเพื่อให้เกิดความชอบด้วยกฎหมาย
- (๒) ห้ามมิให้ใช้ข้อมูลส่วนบุคคลโดยไม่มีเจตนา
- (๓) ห้ามมิให้ใช้ข้อมูลส่วนบุคคลโดยมิได้แจ้งรายละเอียดเอาไว้ในการแจ้งรายละเอียดความเป็นส่วนตัว หรือ Privacy Notice
- (๔) ห้ามมิให้ใช้ข้อมูลส่วนบุคคลนอกจากวัตถุประสงค์ที่ได้ขอความยินยอมไว้จากเจ้าของข้อมูลส่วนบุคคล
- (๕) ห้ามมิให้ใช้ข้อมูลส่วนบุคคลเพื่อการอื่นนอกจากกิจการของบริษัท
- (๖) ห้ามมิให้ทำลาย คัดลอกทำสำเนา เปิดเผย โฆษณาหรือเอาไปเสียซึ่งอุปกรณ์การจัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล
- (๗) เมื่อพนักงานกำหนดระยะเวลาการเก็บข้อมูลส่วนบุคคล ห้ามมิให้ใช้ข้อมูลส่วนบุคคลต่อไป เว้นแต่จะมีกฎหมายกำหนด และให้รายงานผู้บริหาร
- (๘) ห้ามมิให้เข้าถึงข้อมูลส่วนบุคคลที่ถูกควบคุมการเข้าถึง เว้นแต่จะได้รับอนุญาตจากผู้บริหาร

ข้อ ๑๓ การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ให้พนักงานดำเนินการดังนี้

- (๑) ห้ามมิให้ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่อยู่ในความควบคุมของบริษัทโดยไม่ได้รับความยินยอม หรือมีฐานทางกฎหมายรองรับเพื่อความชอบธรรมในการเปิดเผยข้อมูลส่วนบุคคล
- (๒) ห้ามมิให้ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลเพื่อการอื่นนอกเหนือจากวัตถุประสงค์ที่ได้แจ้งเอาไว้ในขณะรวบรวมข้อมูลส่วนบุคคล และดังที่ได้แจ้งเอาไว้ในการแจ้งรายละเอียดความเป็นส่วนตัว หรือ Privacy Notice
- (๓) การใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่ได้รับความยินยอม แต่สามารถอ้างฐานอื่นเพื่อความชอบธรรมได้ ให้ผู้บริหารดำเนินการให้มีการบันทึกการใช้ หรือเปิดเผยเอาไว้ในบันทึกการกิจกรรมข้อมูลส่วนบุคคล หรือ Ropa
- (๔) ห้ามมิให้โอนข้อมูลส่วนบุคคล หรือส่งข้อมูลไปต่างประเทศ เว้นแต่จะได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือมีฐานรองรับเพื่อให้เกิดความชอบธรรม หรือนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบริษัทจะได้รับการตรวจสอบและรับรองจากสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
- (๕) การดำเนินการจะต้องได้รับการอนุญาตจากผู้บริหาร และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
- (๖) ห้ามมิให้เปิดเผยข้อมูลส่วนบุคคลโดยมิได้แจ้งประเภทของบุคคลหรือหน่วยงานเอาไว้ในการแจ้งรายละเอียดความเป็นส่วนตัว หรือ Privacy Notice

(๗) กรณีส่งข้อมูลให้กับบุคคลภายนอกซึ่งอยู่ในราชอาณาจักรเพื่อทำการประมวลผลข้อมูลผู้บริหาร และพนักงานจะต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือมิชอบ ดังนี้

- (ก) จัดทำสัญญาการประมวลผลข้อมูลส่วนบุคคล
- (ข) ตรวจสอบนโยบายการคุ้มครองข้อมูลส่วนบุคคลของบุคคลภายนอกซึ่งเป็นผู้ประมวลผล
- (ค) ผู้ประมวลผลต้องมีการดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลโดยครบถ้วน

ข้อ ๑๔ ให้ผู้บริหาร ดำเนินการบันทึกกิจกรรมการใช้ข้อมูลส่วนบุคคล (Ropa) ให้ถูกต้อง เป็นปัจจุบัน และแจ้งการดำเนินการ หรือปรับปรุงการดำเนินงานให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลทราบ และให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลปรับปรุงข้อมูลในการแจ้งรายละเอียดการใช้ข้อมูลส่วนบุคคลให้ถูกต้องเป็นปัจจุบัน

ข้อ ๑๕ ให้ผู้บริหาร พนักงาน และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลด้วยเหตุดังนี้

- (๑) เมื่อพ้นกำหนดระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล
- (๒) เมื่อไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น

(๓) ตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม เว้นแต่เก็บรักษาไว้เพื่อวัตถุประสงค์ในการใช้เสรีภาพในการแสดงความคิดเห็นการเก็บรักษาไว้เพื่อวัตถุประสงค์ตามที่มีฐานอื่นอันได้แก่

(ก) ข้อมูลทั่วไป ฐานการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือการศึกษาวิจัย หรือฐานป้องกันหรือระงับอันตรายต่อชีวิต ร่างกายหรือสุขภาพ หรือฐานจำเป็นเพื่อปฏิบัติตามสัญญา หรือฐานประโยชน์สาธารณะ หรือฐานประโยชน์อันชอบธรรมของผู้ควบคุมข้อมูลส่วนบุคคล หรือฐานปฏิบัติตามกฎหมาย

(ข) ข้อมูลอ่อนไหว เป็นการจำเป็นในการปฏิบัติตามกฎหมายเพื่อให้บรรลุวัตถุประสงค์เกี่ยวกับ (ก) เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพหรือด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์ ทั้งนี้ ในกรณีที่ไม่ใช่การปฏิบัติตามกฎหมายและข้อมูลส่วนบุคคลนั้นอยู่ในความรับผิดชอบของผู้ประกอบอาชีพหรือวิชาชีพหรือผู้มีหน้าที่รักษาข้อมูลส่วนบุคคลนั้นไว้เป็นความลับตามกฎหมาย ต้องเป็นการปฏิบัติตามสัญญาระหว่างเจ้าของข้อมูลส่วนบุคคลกับผู้ประกอบวิชาชีพทางการแพทย์ (ข) ประโยชน์สาธารณะด้านการสาธารณสุข เช่น การป้องกันด้านสุขภาพจากโรคติดต่ออันตรายหรือโรคระบาดที่อาจติดต่อหรือแพร่เข้ามาใน

ราชอาณาจักร หรือการควบคุมมาตรฐานหรือคุณภาพของยา เวชภัณฑ์ หรือเครื่องมือแพทย์ ซึ่งได้จัดให้มีมาตรการที่เหมาะสมและเจาะจงเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลโดยเฉพาะการรักษาความลับของข้อมูลส่วนบุคคลตามหน้าที่หรือตามจริยธรรมแห่งวิชาชีพ

หมวดที่ ๓

การรักษาความมั่นคงปลอดภัย

ข้อ ๑๖ การรักษาความมั่นคงปลอดภัย เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ ผู้บริหาร และพนักงาน หรือบุคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดต้องดำเนินการให้ครอบคลุมใน ๓ หัวข้อ ดังนี้

- (๑) การเข้ารหัสซึ่งความลับ
- (๒) ความถูกต้อง ครบถ้วน
- (๓) สภาพพร้อมใช้งาน

ข้อ ๑๗ ให้ผู้บริหาร และพนักงาน หรือบุคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดการดำเนินการรักษาความมั่นคงปลอดภัยต้องดำเนินการใน ๓ ด้าน ดังนี้

- (๑) ด้านบริหาร
- (๒) ด้านเทคนิค
- (๓) ด้านกายภาพ

การดำเนินการ อย่างน้อยต้องเป็นไปตามมาตรฐานขั้นต่ำที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

ข้อ ๑๘ การดำเนินการรักษาความมั่นคงปลอดภัยด้านบริหาร ให้ผู้บริหาร และพนักงาน หรือบุคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดดำเนินการดังนี้

- (๑) ผู้บริหาร พนักงานจะต้องดำเนินการตามระเบียบที่เกี่ยวกับการรวบรวม ใช้ และเปิดเผย ในข้อ ๘ ถึงข้อ ๑๕ โดยเคร่งครัด
- (๒) การใช้งาน การเข้าถึงข้อมูลส่วนบุคคล การเข้าพื้นที่ซึ่งมีการเก็บข้อมูลส่วนบุคคลที่ถูกจัดไว้เป็นความลับพนักงานจะต้องมีการขออนุญาตจากผู้บริหารที่ได้รับมอบหมายให้เป็นผู้อนุญาต
- (๓) ให้ผู้บริหารมีการกำหนดรายชื่อพนักงานผู้มีสิทธิเข้าถึงข้อมูลส่วนบุคคล โดยออกเป็นประกาศภายในส่วนงาน

ในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (user responsibilities) ผู้บริหารอาจแบ่งเป็นรูปแบบต่าง ๆ เช่น สิทธิในการเข้าอ่านอย่างเดียว หรือสิทธิในการแก้ไขเพิ่มเติม สิทธิในการเปิดเผยและเผยแพร่ สิทธิในการตรวจสอบคุณภาพข้อมูล สิทธิในการลบทำลาย ทั้งนี้บริษัทจะประกาศให้ทราบต่อไป

(๔) บุคคลตาม (๓) หากจะเข้าถึงข้อมูลเพื่ออ่าน หรือเพื่อแก้ไขเพิ่มเติม หรือเพื่อเปิดเผย และเผยแพร่ หรือตรวจสอบคุณภาพข้อมูล หรือลบทำลายข้อมูล จะกระทำได้อต่อเมื่อได้ขออนุญาตจากผู้บริหาร โดยให้ผู้บริหารตรวจสอบสิทธิตามประกาศ ตรวจสอบว่าการขอใช้สิทธิดังกล่าวมีเหตุอันสมควร และชอบด้วยกฎหมายหรือไม่ หรือการเข้าออกพื้นที่ หรือสถานที่ หรืออุปกรณ์เก็บข้อมูลส่วนบุคคล และให้ลงบันทึกการเข้าใช้งานเอาไว้ ซึ่งการบันทึกอาจทำในรูปกระดาษ หรืออิเล็กทรอนิกส์ก็ได้

(๕) เมื่อมีการเข้าถึงข้อมูลส่วนบุคคลตามข้อ (๔) แล้ว ผู้บริหารจะต้องมีการตรวจสอบ ถูกแก้ไข ถูกคัดลอก หรือ ถูกทำลาย หรือมีการกระทำที่ผิดกฎหมายหรือระเบียบนี้หรือไม่

(๖) ให้พนักงานและบุคลากรทุกคนปฏิบัติตามระเบียบการใช้เทคโนโลยีสารสนเทศอย่างเคร่งครัด

ข้อ ๑๙ การดำเนินการรักษาความมั่นคงปลอดภัยด้านเทคนิค ให้ผู้บริหาร และพนักงาน หรือบุคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดดำเนินการดังนี้

(๑) ให้ฝ่ายเทคโนโลยีสารสนเทศจัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลัง เกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล

(๒) ให้ฝ่ายเทคโนโลยีสารสนเทศการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการใช้งาน ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เผยแพร่ ตลอดจนการลบทำลาย

(๓) ให้ฝ่ายเทคโนโลยีสารสนเทศจัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง โดยดำเนินการทุกกระยะ 1 วัน สำหรับเครื่อง Server backup และดำเนินการเฉพาะวันจันทร์ ถึง ศุกร์ (ยกเว้นวันเสาร์และอาทิตย์) สำหรับเครื่อง Ext. HDD

(๔) ให้ฝ่ายเทคโนโลยีสารสนเทศจัดให้มีระบบการป้องกันการกระทำที่มีชอบด้วยกฎหมายซึ่งข้อมูลส่วนบุคคลโดยใช้เทคโนโลยีที่เหมาะสม เช่น การติดตั้งไฟร์วอลล์แบบมาตรฐาน ระบบปัญญาประดิษฐ์ /AI โปรแกรมแอนตี้ไวรัส และกำหนดสิทธิการเข้าถึงข้อมูล เป็นต้น

(๕) การใช้คอมพิวเตอร์ในพื้นที่ซึ่งมีบุคคลภายนอกสามารถมองเห็นหน้าจอได้ พนักงานจะต้องปรับมุมคอมพิวเตอร์เพื่อป้องกันการมองเห็น รวมถึงการใช้ Screen saver หรือต้องมีการพิกหน้าจอเอาไว้

(๖) เมื่อใช้งานคอมพิวเตอร์ทำงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเสร็จสิ้น ห้ามมิให้พนักงานเก็บข้อมูลเอาไว้ตรงส่วน Desktop จะต้องจัดเก็บข้อมูลเอาไว้ในเครื่องมือ หรืออุปกรณ์ หรือตู้หรือพื้นที่ซึ่งมีระบบป้องกันการเข้าถึง หรือการตั้งรหัสผ่านทุกครั้ง

(๗) การใช้ข้อมูลทางด้านสารสนเทศพนักงานต้องมีการตั้งรหัสผ่าน และเก็บรหัสผ่านเอาไว้ในสถานที่ปลอดภัย และเข้ารหัสไว้ซึ่งความลับ

(๘) ห้ามมิให้พนักงานคัดลอกข้อมูลส่วนบุคคล (Copy) หรือการทำซ้ำข้อมูลไม่ว่าจะผ่านอุปกรณ์ เครื่องมือ โดยไม่ได้รับอนุญาตจากผู้บริหาร

(๙) ห้ามมิให้พนักงานเคลื่อนย้ายข้อมูลผ่านระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตจากผู้บริหาร และการส่งต่อนั้นจะต้องมีการตั้งรหัสผ่านเพื่อป้องกันการเข้าถึง

(๑๐) ห้ามมิให้พนักงานจัดเก็บข้อมูลส่วนบุคคลเอาไว้ในคอมพิวเตอร์ Note Book เว้นแต่คอมพิวเตอร์เครื่องที่ได้รับอนุญาตจากบริษัท ภายใต้เงื่อนไขที่ต้องดูแลคอมพิวเตอร์นั้นเป็นอย่างดี

(๑๑) การใช้คอมพิวเตอร์ส่วนบุคคล Notebook ที่มีข้อมูลสำคัญ พนักงานจะต้องมีการรักษาความมั่นคงปลอดภัยที่มากกว่าคอมพิวเตอร์ทั่วไป เช่น ต้องมีการเข้ารหัส (Encrypted) โดยการกำหนดรหัสแทนชื่อบุคคล รวมถึงมีมาตรการอื่นเสริม เช่น มีการกำหนดรหัสผ่าน (Password)

(๑๒) พนักงานจะต้องจัดเก็บข้อมูลส่วนบุคคลเอาไว้ในพื้นที่ซึ่งบริษัทจัดหาให้ และแจ้งให้พนักงานทราบ

(๑๓) ห้ามมิให้พนักงานจัดเก็บข้อมูลส่วนบุคคลในอุปกรณ์บันทึกข้อมูลแบบพกพา เช่น Hard Disk แบบ External หรือ Flash Drive

(๑๔) กรณีพนักงานการทำงานจากระยะไกล ซึ่งไม่ใช่ที่บริษัทหากจะมีการเข้าระบบคอมพิวเตอร์ จะต้องมีการป้องกันการถูกโจมตีที่เหมาะสม และต้องได้รับอนุญาตจากผู้บริหาร

(๑๕) ห้ามมิให้พนักงานนำอุปกรณ์ต่าง ๆ จากภายนอกมาต่อพ่วงเข้ากับระบบคอมพิวเตอร์ของบริษัท เว้นแต่จะได้รับอนุญาตจากผู้บริหาร

(๑๖) เมื่อมีการพิมพ์งานซึ่งมีข้อมูลส่วนบุคคล พนักงานจะต้องมีการรักษาความปลอดภัย

(๑๗) ห้ามมิให้พนักงานทำการเปลี่ยนแปลงเครือข่าย เช่น IP Address หรืออุปกรณ์อื่นโดยไม่ได้รับอนุญาตจากผู้บริหารของฝ่ายเทคโนโลยีสารสนเทศ

(๑๘) ให้ฝ่ายเทคโนโลยีสารสนเทศทบทวนมาตรการที่เหมาะสมเพื่อป้องกันการสูญหาย การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยีเพื่อให้เกิดประสิทธิภาพในการรักษาความมั่นคงปลอดภัยทางเทคนิคที่เหมาะสม

(๑๙) พนักงานจะต้องปฏิบัติตามระเบียบการใช้เทคโนโลยีสารสนเทศของบริษัทอย่างเคร่งครัด

ข้อ ๒๐ การดำเนินการรักษาความมั่นคงปลอดภัยด้านกายภาพ ให้ผู้บริหาร และพนักงาน หรือบุคคลากรไม่ว่าจะอยู่ในตำแหน่งหรือสถานะใดดำเนินการดังนี้

(๑) ให้ฝ่ายผู้บริหารแต่ละฝ่าย หรือพนักงานแต่ละแผนกจัดให้มีการควบคุมการเข้าถึงข้อมูลส่วนบุคคล และอุปกรณ์ในการจัดเก็บ และประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งาน และความมั่นคงปลอดภัย โดยมีตู้ ซึ่งมีการล็อกกุญแจจัดเก็บข้อมูลส่วนบุคคล หรือมีห้องเก็บเอกสาร หรือมีการติดตั้งกล้อง CCTV หรืออาจมีการกำหนดให้ล้อมรั้ว หรือกำหนดให้ต้องมีบัตรผ่านเข้าออก

(๒) การดำเนินการตามข้อ (๑) หากมีการรวบรวมข้อมูลส่วนบุคคลให้ถือว่าเป็นการดำเนินการโดยอำนาจฐานประโยชน์อันชอบธรรมของบริษัท จึงไม่ต้องขอความยินยอม แต่ให้ดำเนินการตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลให้ถูกต้อง

(๓) การขออนุญาตเข้าถึงข้อมูลส่วนบุคคล ผู้บริหารจะต้องบันทึกการเปิดตู้ หรือการเข้าพื้นที่จัดเก็บข้อมูลเอาไว้

(๔) ในการปฏิบัติงาน กรณีที่มีการทำงานอย่างต่อเนื่อง ซึ่งงานนั้นมีข้อมูลส่วนบุคคล หากปฏิบัติงานนั้นเสร็จแล้ว พนักงานจะต้องมีการจัดเก็บเอกสารหรือข้อมูลนั้นเป็นความลับในทันที ห้ามมิให้วางเอกสารไว้ในที่ใด ๆ ซึ่งไม่มีมาตรการป้องกัน โดยพนักงานจะต้องดำเนินการจัดเก็บเอาไว้ในสถานที่ที่มีการป้องกันการเข้าถึงเชิงกายภาพเอาไว้ เช่น มีตู้ มีกุญแจ มีห้องเก็บเอกสาร มีกล้อง CCTV มีเจ้าหน้าที่ช่วยกันสอดส่องดูแล

หมวดที่ ๔

แจ้งเหตุการละเมิดข้อมูลส่วนบุคคล

ข้อ ๒๑ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเป็นผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่ผู้บริหารสูงสุด หรือผู้ได้รับมอบหมาย พร้อมทั้งแจ้งตัวแทนของสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ทราบโดย การส่งอีเมลล์ แต่ถ้าเป็นจะต้องแจ้งโดยทางโทรศัพท์

ข้อ ๒๒ กรณีความเสียหาย ซึ่งมีผลกระทบต่อสิทธิและเสรีภาพของบุคคลไม่ร้ายแรง เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

กรณีความเสียหายตามวรรคแรก เช่น กรณีมีการรั่วไหลของข้อมูล แต่ปรากฏว่าข้อมูลส่วนบุคคลนั้นถูกเข้ารหัสผ่านเอาไว้ ซึ่งไม่สามารถเปิดอ่าน หรือเข้าถึงได้หากไม่ทราบรหัสผ่าน หรือถูกซอฟต์แวร์เรียกค่าไถ่ (Ransomware) และมีการเปลี่ยนรหัสผ่านทำให้ไม่สามารถใช้งานได้เพื่อเรียกเงินแลกกับการปลดการเข้ารหัสเพื่อให้ใช้ข้อมูลได้ แต่หากไม่ได้ถูกโจรกรรมข้อมูลส่วนบุคคล

อนึ่ง การกระทำดังกล่าวในวรรคแรก หากมีการโจรกรรมข้อมูลส่วนบุคคลให้ถือเป็นความเสี่ยงสูง นอกจากนี้ความเสี่ยงต่ำอาจพิจารณาจากจำนวนผู้เสียหาย จำนวนข้อมูลส่วนบุคคล ความยากง่ายในการเข้าถึงข้อมูลส่วนบุคคลซึ่งมีการกำหนดหรือตั้งค่าการเข้าถึง

กรณีความเสียหายทำให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลดำเนินการเพียงบันทึกเหตุการณ์ไว้เป็นการภายในก็เพียงพอ โดยไม่จำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และไม่จำเป็นต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบ

ข้อ ๒๓ กรณีมีความเสี่ยงสูง ซึ่งอาจกระทบต่อสิทธิและเสรีภาพของบุคคล ผู้โจมตีทำการฝังมัลแวร์หรือไวรัส เพื่อเข้าถึงข้อมูลส่วนบุคคล หรือปริมาณข้อมูลส่วนบุคคลจำนวนมาก ถือว่ามีความเสี่ยงสูงที่เหตุการณ์ดังกล่าวจะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล เช่นนี้ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

บุคคลดำเนินการบันทึกไว้เป็นการภายในถึงการเข้าโจมตี และการโจรกรรมข้อมูล และแจ้งเหตุดังกล่าวโดยไม่ชักช้าภายใน 72 ชั่วโมงนับตั้งแต่ทราบเหตุเท่าที่สามารถทำได้ ไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบ และ ยังต้องแจ้งเจ้าของข้อมูลส่วนบุคคลทราบด้วย

กรณีที่บริษัททำหน้าที่เป็นผู้ประมวลผล ให้แจ้งแก่ผู้ควบคุมข้อมูลส่วนบุคคลถึงเหตุที่มีการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

ข้อ ๒๔ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วน แจ้งการละเมิดต่อเจ้าของข้อมูลส่วนบุคคลให้ทราบ และแจ้งแนวทางการเยียวยาความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ทั้งนี้ ตามความเสียหายที่แท้จริง โดยรายงานไปยังผู้บริหารสูงสุดหรือที่ได้รับมอบหมายเพื่อดำเนินการต่อไป

ข้อ ๒๕ ให้เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลสอบสวนหาสาเหตุการละเมิดข้อมูลส่วนบุคคลในทันทีว่าลักษณะการละเมิดข้อมูลส่วนบุคคลเป็นอย่างไร ประเภทและจำนวนข้อมูลส่วนบุคคลอะไร แหล่งที่เกิดการละเมิดข้อมูลส่วนบุคคลเกิด ณ จุดใด ผลกระทบที่เกิดขึ้นมีอะไรบ้าง และหามาตรการป้องกันที่เหมาะสมในทันที

หมวดที่ ๕

วินัยและโทษทางวินัยของการไม่ปฏิบัติตามระเบียบ

ข้อ ๒๖ พนักงานซึ่งไม่ปฏิบัติตามระเบียบนี้ หรือระเบียบอื่น หรือประกาศนโยบายคุ้มครองข้อมูลส่วนบุคคล หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายลำดับรองที่เกี่ยวข้อง อาจได้รับโทษทางวินัยโดยออกเป็นหนังสือตักเตือน

ข้อ ๒๗ พนักงานซึ่งไม่ปฏิบัติตามระเบียบนี้ หรือระเบียบอื่น หรือประกาศนโยบายคุ้มครองข้อมูลส่วนบุคคล หรือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และกฎหมายลำดับรองที่เกี่ยวข้อง จนเป็นเหตุให้ข้อมูลรั่วไหล หรือนำข้อมูลส่วนบุคคลไปใช้ หรือเปิดเผยต่อบุคคลภายนอกโดยไม่มีหน้าที่ หรือไม่ได้รับอนุญาตให้เข้าถึงข้อมูลส่วนบุคคล อาจได้รับโทษทางวินัยในระดับการออกหนังสือตักเตือน

อนึ่ง หากการดำเนินการฝ่าฝืนระเบียบตามวรรคแรกเป็นเหตุให้เกิดการรั่วไหลของข้อมูลส่วนบุคคล จนเกิดความเสียหายสูง พนักงานอาจได้รับโทษถึงขั้นเลิกจ้างโดยไม่จ่ายค่าชดเชย รวมถึงอาจต้องรับผิดชอบทางแพ่ง อาญา และทางปกครอง

ทั้งนี้ ระเบียบนี้ให้มีผลบังคับใช้ตั้งแต่วันที่ ๑ เดือน มิถุนายน พ.ศ. ๒๕๖๕ เป็นต้นไป

ประกาศ ณ วันที่ ๓๐ เดือน พฤษภาคม พ.ศ. ๒๕๖๕

ลงชื่อ

(นางสาวรุ่งรัตน์ ศิริรัตนพานิชย์)

กรรมการผู้จัดการ

บริษัท แม่น้ำสแตนเลสไวร์ จำกัด (มหาชน)