SIAMESE ASSET
ASSET OF LIFE

มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล
บริษัท ไซมิส แอสเสท จำกัด (มหาชน)

---

1. **<u>หลักการและเหตุผล</u>**

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลส่วนบุคคล ทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ โดยพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่องมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 (“กฎหมาย”) กำหนดหน้าที่ให้ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

วัตถุประสงค์ของการรักษาความปลอดภัยเพื่อคุ้มครองสิทธิในความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคล และอำนาจในการควบคุมข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งกฎหมายรับรองไว้ให้ ด้วยเหตุนี้ การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลเป็นหน้าที่ตามกฎหมายที่ผู้ควบคุมข้อมูลส่วนบุคคล (รวมถึงผู้ประมวลผลข้อมูลส่วนบุคคล) ต้องปฏิบัติเพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ซึ่งอาจนำไปสู่การละเมิดข้อมูลส่วนบุคคล

2. **<u>การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล</u>**

บริษัทจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลโดยครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลตามกฎหมาย ทั้งมาตรการป้องกันด้านการบริหารจัดการ มาตรการป้องกันด้านเทคนิค และมาตรการป้องกันทางกายภาพ โดยดำเนินการดังนี้

<u>2.1) มาตรการป้องกันด้านการบริหารจัดการ</u>

2.1.1) แจ้งมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลตามนโยบายนี้ให้แก่คณะกรรมการ กรรมการผู้บริหาร พนักงานหรือผู้ปฏิบัติงานทุกระดับ และลูกจ้างทุกประเภทของบริษัท ตลอดจนคู่ค้า พันธมิตรทางธุรกิจ และ/หรือผู้มีส่วนได้เสียของบริษัททราบ รวมถึงสร้างเสริมความตระหนักรู้ด้านความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลให้กับกลุ่มบุคคลดังกล่าวปฏิบัติตามมาตรการที่กำหนดอย่างเคร่งครัด

2.1.2) ระบุความเสี่ยงที่อาจเกิดขึ้นกับทรัพย์สินสารสนเทศ การป้องกันความเสี่ยงที่อาจเกิดขึ้นการตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยเป็นไปตามนโยบายการรักษาความปลอดภัยทางสารสนเทศ กำหนดหน้าที่รับผิดชอบให้แก่ตัวแทนบริษัทในการดำเนินการเมื่อเกิดเหตุละเมิด และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามและเหตุการณ์ละเมิดข้อมูลส่วนบุคคล ดังนี้

2.1.2.1) กำหนดตัวพนักงานผู้รับผิดชอบกิจกรรมและวิธีการแจ้งเหตุละเมิดให้แก่ตัวแทนของบริษัทให้ชัดเจน เช่น การส่งอีเมล และแจ้งทางโทรศัพท์ในกรณีเหตุละเมิดที่มีความรุนแรงและเร่งด่วน

2.1.2.2) กำหนดวิธีปฏิบัติให้ตัวแทนของบริษัทต้องดำเนินการแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุ

2.1.2.3) การแจ้งเหตุละเมิดตามข้อ 2.1.2.2) อาจได้รับยกเว้นหากไม่มีความเสี่ยงที่จะมีผลกระทบต่อสิทธิและเสรีภาพของบุคคล ทั้งนี้ เมื่อมีเหตุการณ์ละเมิดข้อมูลส่วนบุคคล บริษัทต้องทบทวนมาตรการรักษาความมั่นคงปลอดภัยทุกครั้ง

2.1.3) กำหนดการอนุญาตหรือการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน (User Responsibilities) แบ่งเป็นรูปแบบต่าง ๆ เช่น สิทธิในการเข้าดู แก้ไข เพิ่มเติม เปิดเผยและเผยแพร่ การตรวจสอบคุณภาพข้อมูล ตลอดจนการลบทำลาย

2.1.4) บริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาตแล้ว

2.1.5) การจัดการเข้าถึงสารสนเทศ (Information Access Restriction)การเข้าถึงสารสนเทศและฟังก์ชันในระบบงานต้องมีการจำกัดให้สอดคล้องกับนโยบายควบคุมการเข้าถึง ผู้ดูแลระบบ ต้องจัดการให้ระบบแสดงข้อความเตือนถึง “การอนุญาตให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้นที่มีสิทธิ์เข้าใช้งาน ” ก่อนที่จะทำการเชื่อมต่อเข้าสู่ระบบคอมพิวเตอร์ขององค์กร และระบบต้องเปิดโอกาสให้ผู้ใช้สามารถยกเลิกการเชื่อมต่อเข้าสู่ระบบในกรณีที่ทราบว่าระบบนั้น ๆ ไม่ได้เกี่ยวข้องกับตนเอง

- ผู้ใช้ทุกคนต้องมีรหัสผู้ใช้ (User-ID) เฉพาะบุคคล เพื่อสามารถระบุและติดตามการใช้งานของผู้ใช้ แต่ละคนได้ ซึ่งรหัสผู้ใช้เป็นรหัสเฉพาะบุคคล โดยไม่มีการใช้รหัสผู้ใช้ร่วมกัน (Shared User ID)

- รหัสผ่านสำหรับการเข้าสู่ระบบถือเป็นความลับ ผู้ใช้ต้องไม่แบ่งปันหรือเปิดเผยรหัสผู้ใช้ของตน ให้บุคคลอื่น ในกรณีที่พนักงานลาออก รหัสผู้ใช้รายนั้นต้องไม่ถูกนำกลับมาใช้ใหม่

- ผู้ใช้ต้องออกจากระบบเครือข่าย (Log-off) ทันที เมื่อใช้งานเสร็จหรือไม่มีความจำเป็นต้องใช้งานอีก

- ผู้ใช้ถูกติดตั้งโปรแกรมถนอมหน้าจอ (Screen Saver) ที่มีรหัสผ่านบนเครื่องคอมพิวเตอร์ โดยโปรแกรมเหล่านี้จะเริ่มทำงานหลังจากไม่มีการใช้งานใด ๆ บนเครื่องคอมพิวเตอร์นั้น ๆ ตามเวลาที่กำหนดไว้

- หากไม่มีการใช้งานเป็นเวลานาน ผู้ใช้ต้องปิดเครื่องคอมพิวเตอร์ หรือเครื่องปลายทางให้เรียบร้อย

2.1.5) จัดให้มีวิธีการเพื่อตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล

2.1.6) ในกรณีที่มีการฝ่าฝืนไม่ปฏิบัติตามมาตรการรักษาความมั่นคงปลอดภัยนี้เนื่องจากความบกพร่องของบริษัท และทำให้เกิดการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคล บริษัทจะแจ้งให้เจ้าของข้อมูลทราบถึงรายละเอียดของเหตุการณ์และแผนเยียวยาความเสียหายจากการละเมิดหรือรั่วไหลดังกล่าวโดยเร็ว อย่างไรก็ตาม บริษัทจะไม่รับผิดชอบในความเสียหายใด ๆ อันเกิดจากการใช้ การเปิดเผย รวมถึงการประมาทเลินเล่อของเจ้าของข้อมูลหรือบุคคลอื่นที่ได้รับความยินยอมจากเจ้าของข้อมูล

2.1.7) เมื่อพ้นระยะเวลาการใช้งานข้อมูลส่วนบุคคลหรือไม่มีความจำเป็นในการเก็บรักษาข้อมูลส่วนบุคคลอีกต่อไป บริษัทจะลบหรือทำลายข้อมูลส่วนบุคคลออกจากระบบการจัดเก็บ เว้นแต่ในกรณีที่ต้องเก็บรักษาข้อมูลส่วนบุคคลไว้ตามที่กฎหมายกำหนด

2.1.8) บริษัทมีการดำเนินการสอบทานและประเมินประสิทธิภาพของระบบรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคลโดยหน่วยงานตรวจสอบภายใน

2.2) มาตรการป้องกันด้านเทคนิค

2.2.1) จัดให้มีวิธีการเพื่อให้สามารถตรวจสอบย้อนหลังเกี่ยวกับการเข้าถึง เปลี่ยนแปลง ลบ หรือถ่ายโอนข้อมูลส่วนบุคคล ให้สอดคล้องเหมาะสมกับวิธีการและสื่อที่ใช้ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

2.2.2) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลเฉพาะผู้ที่ได้รับอนุญาต ตามระดับสิทธิการจัดการข้อมูล ได้แก่ การนำเข้า เปลี่ยนแปลง แก้ไข เปิดเผย ตลอดจนการลบทำลาย ซึ่งรวมถึงแต่ไม่จำกัดเพียง

2.2.2.1) การควบคุมการเข้าถึงข้อมูลส่วนบุคคล ต้องมีการยืนยันตัวตนและการอนุญาตให้เข้าถึงอย่างเหมาะสม โดยจะต้องให้สิทธิในการเข้าถึงเฉพาะในสิ่งที่จำเป็นเท่านั้น ช่วยป้องกันการเข้าถึงข้อมูลโดยไม่จำเป็น

2.2.2.2) การบริหารจัดการการเข้าถึงของผู้ใช้งานควรมีขั้นตอนที่เหมาะสม เช่น การลงทะเบียนและถอนสิทธิผู้ใช้งาน การจัดการสิทธิในการเข้าถึงข้อมูล การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตน และการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ รวมถึงการปรับปรุงหรือถอดถอนสิทธิการเข้าถึงเมื่อจำเป็น เพื่อให้การควบคุมการเข้าถึงเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2.2.3) การจัดให้มีระบบสำรองและกู้คืนข้อมูล เพื่อให้ระบบ และ/หรือ บริการต่าง ๆ ยังสามารถดำเนินการได้อย่างต่อเนื่อง ทั้งนี้เป็นไปตามหลักเกณฑ์และวิธีปฏิบัติทางสารสนเทศของบริษัท

2.3.4) มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Controls against Malware) มาตรการตรวจหา การป้องกัน และการกู้คืน จากโปรแกรมไม่ประสงค์ดี ต้องมีการดำเนินการร่วมกับการสร้างความตระหนักผู้ใช้งานที่เหมาะสม

- หน่วยงานเทคโนโลยีสารสนเทศ จัดให้มีการติดตั้งโปรแกรมป้องกัน Virus Version ล่าสุดในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์ทุกเครื่อง และเครื่อง Server โดยมีการ Update ให้ทันสมัยอยู่ตลอดเวลา

- หน่วยงานเทคโนโลยีสารสนเทศ กำหนดให้โปรแกรมค้นหา Virus ทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะการใช้ระบบด้วย

- ไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตมีการตรวจหา Virus ก่อนนำไปใช้งาน

- ห้ามพนักงานดำเนินการใด ๆ ที่เกี่ยวกับการพัฒนา Virus หรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ

- ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกที่อนุญาตให้นำมาใช้ ผู้ที่จะใช้งานสื่อข้อมูลนั้นต้องตรวจสอบ Virus คอมพิวเตอร์ก่อนใช้งานทุกครั้ง

2.3) มาตรการป้องกันทางกายภาพ

2.3.1) การควบคุมการเข้าถึงข้อมูลส่วนบุคคลและอุปกรณ์ในการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย เช่น มีเจ้าหน้าที่รักษาความปลอดภัยของพื้นที่ มีระบบกล้องวงจรปิดติดตั้ง และมีการล็อกตู้เก็บเอกสารข้อมูลส่วนบุคคล เป็นต้น ทั้งนี้ความเข้มข้นของมาตรการให้เป็นไปตามระดับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล

2.3.2) การกำหนดผู้ที่ได้รับอนุญาตให้เข้าถึงอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคลตามหน้าที่ความรับผิดชอบ เพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต เปิดเผย ล่วงรู้ หรือลักลอบทำสำเนาข้อมูลส่วนบุคคล ลักขโมยอุปกรณ์จัดเก็บหรือประมวลผลข้อมูลส่วนบุคคล ลักลอบนำอุปกรณ์เข้าออก การดำเนินการป้องกันและระมัดระวังไม่ให้

ข้อมูลรั่วไหลหรือถูกละเมิดอย่างหนึ่งอย่างใด เช่น ไม่เปิดไฟล์ข้อมูลส่วนบุคคลในที่สาธารณะ ปิด/เก็บข้อมูลส่วนบุคคลให้มิดชิดเมื่อลุกออกจากโต๊ะ เป็นต้น

2.3.3) ข้อห้ามในการใช้งานสื่อบันทึกข้อมูล:

- ห้ามพนักงานทุกคนใช้งานสื่อบันทึกข้อมูลใด ๆ ทั้งภายในและภายนอกบริษัท เช่น USB แฟลชไดรฟ์ , ฮาร์ดไดรฟ์แบบพกพา, การ์ดหน่วยความจำ, CD และ DVD โดยเด็ดขาด

- ห้ามพนักงานนำสื่อบันทึกข้อมูลส่วนตัวมาใช้ในคอมพิวเตอร์หรืออุปกรณ์ของบริษัท รวมถึงการนำสื่อบันทึกข้อมูลของบริษัทไปใช้ในอุปกรณ์ส่วนตัว

2.3.4) การควบคุมการเชื่อมต่อสื่อบันทึกข้อมูล

- หน่วยงานเทคโนโลยีสารสนเทศ ตั้งค่าระบบให้มีการบล็อกการเชื่อมต่อสื่อบันทึกข้อมูลทั้งหมดในอุปกรณ์คอมพิวเตอร์ของบริษัท เพื่อป้องกันการใช้งานโดยไม่ได้รับอนุญาต

- ในกรณีที่มีความจำเป็นต้องใช้สื่อบันทึกข้อมูล ฝ่าย IT จะเป็นผู้อนุมัติและดำเนินการถ่ายโอนข้อมูลด้วยวิธีการที่ปลอดภัยตามขั้นตอนที่กำหนดไว้

2.3.5) ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical Security Perimeter) ต้องจัดห้อง Server ที่มีสภาพแวดล้อมภายนอกปลอดภัยจากภัยคุกคามภายนอก คือ อยู่ในสถานที่ ๆ เข้าถึงได้โดยยากจากบุคคลภายนอก อยู่บนอาคารสูงที่สามารถป้องกันเหตุจากน้ำท่วมได้ และห้องระบบคอมพิวเตอร์ต้องติดตั้งระบบประตูอัตโนมัติ ที่สามารถปิดทันทีโดยอัตโนมัติหลังจากที่เปิดประตูแล้ว และจะต้องมีสัญญาณเตือนเมื่อมีการเปิดประตูทิ้งไว้

2.4) ข้อตกลงระหว่างบริษัทและผู้ประมวลผลข้อมูลส่วนบุคคล

กรณีมีข้อตกลงระหว่างบริษัทและผู้ประมวลผลข้อมูลส่วนบุคคล บริษัทจะกำหนดให้ผู้ประมวลผลข้อมูลส่วนบุคคลจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเทียบเท่าหรือดีกว่ามาตรการตามนโยบายนี้ เพื่อป้องกันการสูญหาย การเข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ หรือกระทำโดยปราศจากอำนาจโดยชอบด้วยกฎหมาย รวมทั้งแจ้งให้บริษัททราบถึงเหตุการณ์ละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น ทั้งนี้ความเข้มข้นของมาตรการให้เป็นไปตามระดับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้นหากข้อมูลส่วนบุคคลรั่วไหล ถูกแก้ไข ถูกคัดลอก หรือถูกทำลายโดยมิชอบ

2.5) การส่ง การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ

การส่ง การโอนข้อมูลส่วนบุคคลไปยังต่างประเทศ รวมถึงการนำข้อมูลส่วนบุคคลไปเก็บบนฐานข้อมูลในระบบอื่นใดซึ่งผู้ให้บริการรับโอนข้อมูลหรือบริการเก็บรักษาข้อมูลอยู่ต่างประเทศ ประเทศปลายทางที่เก็บรักษาข้อมูลต้องมีมาตรการคุ้มครองข้อมูลส่วนบุคคลที่เทียบเท่าหรือดีกว่ามาตรการตามนโยบายนี้

2.6) การฝ่าฝืนมาตรการการรักษาความมั่นคงปลอดภัยของบริษัท

ในกรณีที่มีการฝ่าฝืนมาตรการรักษาความมั่นคงปลอดภัยของบริษัทจนเป็นเหตุให้มีการละเมิดข้อมูลส่วนบุคคล หรือข้อมูลส่วนบุคคลรั่วไหลสู่สาธารณะ บริษัทจะดำเนินการแจ้งเจ้าของข้อมูลให้ทราบโดยเร็ว รวมทั้งแจ้งแผนการเยียวยาความเสียหายจากการละเมิดหรือการรั่วไหลของข้อมูลส่วนบุคคลสู่สาธารณะในกรณีที่เกิดจากความบกพร่องของบริษัท

3. **<u>การทบทวนมาตรการ</u>**

บริษัทต้องจัดให้มีการทบทวนมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคลฉบับนี้เป็นประจำทุกปี เมื่อมีความจำเป็น และ/หรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป

4. **<u>คำสงวนสิทธิ</u>**

บริษัทจะไม่รับผิดชอบกรณีที่ความเสียหายใดๆ อันเกิดจากการใช้หรือการเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่สาม รวมถึงการละเลยหรือเพิกเฉย การออกจากระบบ (Log Out) ฐานข้อมูลหรือระบบสื่อสารสังคมออนไลน์ของบริษัท โดยการกระทำของเจ้าของข้อมูลหรือบุคคลอื่นซึ่งได้รับความยินยอมจากเจ้าของข้อมูล

หมายเหตุ แนวปฏิบัติสำหรับการดำเนินการของผู้ควบคุมข้อมูลส่วนบุคคลเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ดำเนินการภายใต้**นโยบายรักษาความปลอดภัยสารสนเทศ** ของ บริษัท ไซมิส แอสเสท จำกัด (มหาชน)

ประกาศ ณ วันที่ 1 มิถุนายน พ.ศ. 2567 เป็นต้นไป

บริษัท ไซมิส แอสเสท จำกัด (มหาชน)