
นโยบายความปลอดภัยสารสนเทศ

(Information Security Policy)

ฉบับปรับปรุงครั้งที่ 1 (1 มีนาคม 2565)

บริษัท สิงห์ เอสเตท จำกัด (มหาชน)

จัดทำโดย	ฝ่ายเทคโนโลยีสารสนเทศ
เห็นชอบโดย	คณะกรรมการบริหาร
อนุมัติโดย	คณะกรรมการบริษัท

สารบัญ

1. บทนำ.....	4
2. ความจำเป็นของนโยบาย.....	4
3. วัตถุประสงค์.....	4
4. ขอบเขตการบังคับใช้นโยบาย	5
5. บทบาท.....	5
6. รายละเอียดนโยบายความปลอดภัยสารสนเทศ.....	6
7. การทบทวนและดูแลนโยบาย.....	7
8. การละเมิดฝ่าฝืน.....	7

1. บทนำ

เนื่องด้วยปัจจุบัน บริษัท สิงห์ เอสเตท จำกัด (มหาชน) และบริษัทย่อย (“บริษัทฯ”) ได้มีการใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการดำเนินงานของบริษัทฯ ทั้งในส่วนของระบบงานต่างๆจนถึงการให้บริการลูกค้า ซึ่งระบบและข้อมูลสารสนเทศไม่ว่าในรูปแบบไฟล์ ฐานข้อมูล เอกสารหรืออื่น ๆ ถือเป็นทรัพย์สินอันสำคัญยิ่งของบริษัทฯ ประกอบกับบริษัทฯ ต้องดำเนินธุรกิจภายใต้กฎหมาย ข้อบังคับจากหน่วยงานกำกับของรัฐ และภาวะผูกพันในสัญญาอันเกี่ยวเนื่องกับ ความปลอดภัยสารสนเทศ เพื่อให้มั่นใจว่าระบบและข้อมูลสารสนเทศมีการสร้าง จัดเก็บ ใช้งาน เปิดเผย ปรับปรุงแก้ไข รับส่ง หรือทำลายอย่างปลอดภัยเหมาะสมกับข้อมูลนั้น ๆ ดังนั้น เพื่อเป็นการรักษาความลับ ความถูกต้อง สมบูรณ์ และความพร้อมใช้ของระบบและข้อมูลสารสนเทศ อันจะทำให้ลดความเสี่ยงของบริษัทฯ และผู้ใช้งาน เกี่ยวกับ ความปลอดภัยสารสนเทศ บริษัทฯ จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการควบคุมการดำเนินการใด ๆ กับระบบและข้อมูลสารสนเทศด้วยการสนับสนุนอย่างเต็มที่จากฝ่ายบริหารของบริษัทฯ นโยบายความปลอดภัยสารสนเทศของบริษัทฯ (“นโยบายฯ”) ถูกจัดทำขึ้นเพื่อแสดงเจตจำนงและยุทธศาสตร์ของบริษัทฯ ในด้านความปลอดภัยสารสนเทศเพื่อบริหารจัดการ ด้านความปลอดภัยสารสนเทศที่เหมาะสมกับธุรกิจและวัฒนธรรมของบริษัทฯ

2. ความจำเป็นของนโยบายฯ

บริษัทฯ มีความเสี่ยงหลากหลายจากทั้งภายนอกและภายใน รวมทั้งมีความรับผิดชอบในการรักษาความปลอดภัยสารสนเทศ ระบบสารสนเทศ และทรัพย์สินของบริษัทฯ ตามกฎหมายข้อบังคับ และภาวะผูกพันในสัญญา ซึ่งความเสี่ยงดังกล่าวถือเป็นตัวหลักต้นสำคัญถึงความจำเป็นของนโยบาย นอกจากนี้ความเชื่อมั่นในความปลอดภัยของสารสนเทศซึ่งมีความสำคัญอย่างยิ่งในการดำเนินธุรกิจ ไม่ว่าจะเป็นการเปิดเผยสารสนเทศโดยไม่เหมาะสม ความคลาดเคลื่อน ไม่สมบูรณ์ หรือไม่พร้อมใช้งานของสารสนเทศที่สำคัญอาจสร้างความเสียหายให้กับธุรกิจของบริษัทฯ ได้ ดังนั้น หากปราศจากนโยบายที่ชัดเจนและมีการควบคุมบังคับใช้ที่ดี บริษัทฯจะขาดทิศทางในการจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศและอาจสร้างความเสียหายอย่างรุนแรงกับบริษัทฯ

3. วัตถุประสงค์

เพื่อดำเนินการบริหารจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศอย่างเหมาะสมกับธุรกิจของบริษัทฯ ตามแนวทางมาตรฐานสากล ในการปกป้องทรัพย์สินสารสนเทศของบริษัทฯ รวมถึงของลูกค้า บุคคลและหน่วยงานภายนอกอื่น ๆ ที่อยู่ในการดูแลรับผิดชอบของบริษัทฯ จากภัยคุกคามต่าง ๆ ทั้งจากภายในและภายนอก ทั้งโดยเจตนาและไม่เจตนา เพื่อให้เป็นไปตามกฎหมายและข้อบังคับต่าง ๆ ที่เกี่ยวข้องอย่างถูกต้อง เช่น

- พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พรบ. คุ้มครองข้อมูลส่วนบุคคล
- กฎหมายธุรกรรมอิเล็กทรอนิกส์
- กฎหมายลิขสิทธิ์ และสิทธิบัตร
- ข้อบังคับจากหน่วยงานของรัฐ

- ภาวะผูกพันในสัญญา และความรับผิดชอบต่อลูกค้า บุคคลภายนอกและ หน่วยงานภายนอกที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

4. ขอบเขตการบังคับใช้นโยบาย

นโยบายความปลอดภัยสารสนเทศฉบับนี้บังคับใช้กับกรรมการ ผู้บริหาร และพนักงานของบริษัท สิงห์ เอสเตท จำกัด (มหาชน) รวมถึงบริษัทย่อยและบริษัทร่วมของบริษัทฯ หากไม่มีนโยบายเรื่องนี้ที่กำหนดเป็นอย่างอื่น

5. บทบาท

บริษัทฯ กำหนดโครงสร้างการกำกับดูแลให้การดำเนินงานเป็นไปโดยสอดคล้องกับนโยบายนี้ ดังนี้

หน่วยงาน/บุคคลากรผู้ปฏิบัติหน้าที่	หน้าที่ และความรับผิดชอบ
ผู้ใช้ทุกคน	ผู้ใช้ทุกคนที่อยู่ภายใต้การบังคับใช้ของนโยบายฯ ต้องปฏิบัติตามนโยบายฯ และมาตรการต่าง ๆ ของบริษัทฯ นอกจากนี้ผู้ใช้ต้องรายงานเหตุการณ์สิ่งผิดปกติ จุดอ่อนและช่องโหว่ต่าง ๆ ที่พบเกี่ยวกับความปลอดภัยสารสนเทศ ให้กับแผนก IT
ผู้บังคับบัญชา	<ul style="list-style-type: none"> • ผลักดัน สนับสนุนและทบทวนการปฏิบัติงานและมาตรการต่าง ๆ ในขอบเขตความรับผิดชอบให้สอดคล้องกับกฎหมาย ข้อบังคับ และนโยบายบริษัทฯ • สื่อสารนโยบายและมาตรการต่าง ๆ ให้กับพนักงานและบุคคลภายใต้ขอบเขตความรับผิดชอบ • ดำเนินการให้พนักงานทุกคนในสังกัดได้รับการอบรมและมีความตระหนักรู้ด้านความปลอดภัยสารสนเทศอย่างเพียงพอที่จะรู้เท่าทันภัยและช่องโหว่ต่าง ๆ ในการปฏิบัติงานและการใช้งานระบบสารสนเทศ
เจ้าของระบบ/ข้อมูลทางธุรกิจ	<p>ทุกระบบ ข้อมูลสารสนเทศ หรือทรัพย์สินประเภทอื่น ๆ ต้องมีเจ้าของที่รับผิดชอบชัดเจน โดยเจ้าของต้อง</p> <ul style="list-style-type: none"> • ประเมินความเสี่ยงและผลกระทบทางธุรกิจของระบบและข้อมูลสารสนเทศ • อนุมัติยอมรับความเสี่ยงที่เหลือจากใช้มาตรการ • แบ่งระดับชั้นความปลอดภัยข้อมูล (classify) และสิทธิการใช้งานในระบบตามตำแหน่งงาน หรือหน้าที่การปฏิบัติงาน สำหรับข้อมูลสารสนเทศในความรับผิดชอบ • ดำเนินการให้มั่นใจว่าระบบและข้อมูลในความรับผิดชอบได้รับการปกป้องตามความต้องการที่กำหนด

หน่วยงาน/บุคคลากรผู้ปฏิบัติหน้าที่	หน้าที่ และความรับผิดชอบ
	<ul style="list-style-type: none"> • ทบทวนประสิทธิผลของมาตรการที่จัดทำไป • กำหนดความต้องการสำหรับระบบและข้อมูลเพื่อความต่อเนื่องทางธุรกิจ เช่น การสำรอง การกู้คืนระบบ
ผู้ควบคุมข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลที่ได้รับ จัดเก็บ ประมวลผล ส่งต่อ และทำลาย ต้องมีผู้ควบคุมข้อมูลที่รับผิดชอบชัดเจน โดยผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ควบคุมการบริหารจัดการข้อมูลส่วนบุคคลให้เป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลและนโยบายความปลอดภัยสารสนเทศนี้
แผนก IT	<ul style="list-style-type: none"> • สนับสนุนงานปฏิบัติการระบบให้กับเจ้าของระบบ/ข้อมูล • ให้คำแนะนำทางเทคนิคกับเจ้าของระบบ/ข้อมูลในการกำหนดความต้องการและเลือกมาตรการการควบคุมที่เหมาะสม • จัดทำรายงานและให้ข้อมูลทางเทคนิคเกี่ยวกับภัยช่องโหว่และมาตรการต่าง ๆ

5. นโยบายความปลอดภัยสารสนเทศ

- ททรัพย์สินข้อมูลสารสนเทศต้องถูกปกป้องตามระดับความปลอดภัยที่กำหนด โดยให้เข้าถึงได้เฉพาะเท่าที่จำเป็นในการดำเนินธุรกิจ หรือบทบังคับทางกฎหมาย
- หน่วยงานต้องดำเนินกิจกรรมกับระบบและข้อมูลสารสนเทศทุกรูปแบบ โดยยึดหลักตาม"มาตรฐานความปลอดภัยสารสนเทศ"ของบริษัทฯ เป็นอย่างน้อย
- พนักงานทุกคนต้องปฏิบัติตามกฎหมายและข้อบังคับต่างๆที่เกี่ยวข้อง รวมถึงนโยบายของบริษัทฯอย่างเคร่งครัด
- พนักงานทุกคนต้องรับผิดชอบในการดำเนินกิจกรรมกับข้อมูลสารสนเทศเพื่อธุรกิจของบริษัทฯเท่านั้นภายในขอบเขต ความรับผิดชอบของตน
- ผู้บังคับบัญชาต้องดำเนินการให้มั่นใจได้ว่ามาตรการต่าง ๆ ที่ถูกจัดทำขึ้นต้องสอดคล้องกับนโยบายความปลอดภัยสารสนเทศของบริษัทฯ
- มีการสื่อสาร เพื่อให้มีความรู้ความเข้าใจถึงนโยบายและระเบียบปฏิบัติด้านความปลอดภัยสารสนเทศของบริษัทฯ แก่พนักงานและบุคคลภายนอกที่เกี่ยวข้อง
- ข้อมูลสารสนเทศและระบบต่าง ๆ ต้องถูกกำหนดเจ้าของและความรับผิดชอบที่ชัดเจน
- ระบบต่างๆต้องได้รับการออกแบบให้มีการควบคุม หรือป้องกันข้อมูลสารสนเทศตามที่กฎหมายกำหนด
- ต้องมีการตรวจสอบการปฏิบัติงานและระบบเพื่อความปลอดภัยกับนโยบายและบทบังคับต่าง ๆ โดยผู้ตรวจสอบประเมินอิสระที่ได้รับอนุญาตจากบริษัทฯ

นโยบายดังกล่าวถือเป็นส่วนหนึ่งของแนวปฏิบัติในการดำเนินงานของบริษัทฯ (Code of Conduct) เพื่อความสอดคล้องกับกฎหมายและความรับผิดชอบของบริษัทฯที่มีต่อพนักงานและลูกค้า

7. การทบทวนและดูแลนโยบายฯ

นโยบาย ระเบียบ และข้อปฏิบัติต่าง ๆ ต้องถูกทบทวนอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้งหรือ เมื่อมีการเปลี่ยนแปลงหรือเหตุการณ์สำคัญ เช่น บทบังคับใหม่ตามกฎหมาย พบจุดอ่อนที่สำคัญนโยบายและมาตรฐานอยู่ภายใต้การควบคุมเอกสาร (document control) ซึ่งต้องถูกจัดเก็บอย่างปลอดภัยตามมาตรฐานของบริษัทฯ

8. การละเมิดฝ่าฝืน

การไม่ปฏิบัติตามนโยบายความปลอดภัยสารสนเทศ บริษัทฯ มีสิทธิในการพิจารณาลงโทษตามข้อบังคับเกี่ยวกับการทำงานของบริษัท

ประกาศเมื่อ 24 กุมภาพันธ์ 2566

(นายปิติพงศ์ พิ้งบุญ ณ อยุธยา)

ประธานกรรมการ

บริษัท สิงห์ เอสเตท จำกัด (มหาชน)