นโยบายความปลอดภัยเทคโนโลยีสารสนเทศ

บริษัทฯ เอส โฮเทล แอนด์ รีสอร์ท จำกัด (มหาชน)

1. บทนำ

เนื่องด้วยปัจจุบัน บริษัทฯ เอส โฮเทล แอนด์ รีสอร์ท จำกัด (มหาชน) และบริษัทฯ ย่อย (“บริษัทฯ”) ได้มีการใช้เทคโนโลยีสารสนเทศ ในการดำเนินงานของบริษัทฯ ทั้งในส่วนของระบบงานต่างๆจนถึงการให้บริการลูกค้า ซึ่งระบบสารสนเทศไม่ว่าในรูปแบบไฟล์ ฐานข้อมูล เอกสารหรืออื่น ๆ ถือเป็นทรัพย์สินอันสำคัญยิ่งของบริษัทฯ บริษัทฯ ต้องดำเนินธุรกิจภายใต้กฎหมาย ข้อบังคับจากหน่วยงานกำกับของรัฐ และภาระผูกพันในสัญญาอันเกี่ยวเนื่องกับความปลอดภัยสารสนเทศเพื่อให้มั่นใจว่าระบบและข้อมูลสารสนเทศมีการสร้าง จัดเก็บ ใช้งาน เปิดเผย ปรับปรุงแก้ไข รับส่ง หรือทำลายอย่างปลอดภัยเหมาะสมกับข้อมูลนั้น ๆ ดังนั้นเพื่อเป็นการรักษาความลับ ความถูกต้องสมบูรณ์ และความพร้อมใช้ของระบบและข้อมูลสารสนเทศอันจะทำให้ลดความเสี่ยงของบริษัทฯ และผู้ใช้งาน เกี่ยวกับความปลอดภัยสารสนเทศบริษัทฯ จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการควบคุมการดำเนินการใดกับระบบและข้อมูลสารสนเทศด้วยการสนับสนุนอย่างเต็มที่จากฝ่ายบริหารของบริษัทฯ นโยบายความปลอดภัยสารสนเทศของบริษัทฯ (“นโยบาย”) ถูกจัดทำขึ้นเพื่อแสดงเจตน์จำนงและยุทธศาสตร์ของบริษัทฯ ในด้านความปลอดภัยด้านสารสนเทศเพื่อบริหารจัดการด้านความปลอดภัยสารสนเทศที่เหมาะสมกับธุรกิจและวัฒนธรรมของบริษัทฯ

2. ความจำเป็นของนโยบายฯ

บริษัทฯ มีความเสี่ยงหลากหลายจากทั้งภายนอกและภายในรวมทั้งมีความรับผิดชอบในการรักษาความปลอดภัยของระบบสารสนเทศและทรัพย์สินของบริษัทฯ ตามกฎหมายข้อบังคับและภาระผูกพันในสัญญาซึ่งความเสี่ยงดังกล่าวถือเป็นตัวผลักดันสำคัญถึงความจำเป็นของนโยบาย นอกจากนี้ความเชื่อมั่นในความปลอดภัยของสารสนเทศซึ่งมีความสำคัญอย่างยิ่งในการดำเนินธุรกิจไม่ว่าจะเป็นการเปิดเผยสารสนเทศโดยไม่เหมาะสม ไม่สมบูรณ์หรือไม่พร้อมใช้งานของสารสนเทศที่สำคัญอาจสร้างความเสียหายให้กับธุรกิจของบริษัทฯ ได้ ดังนั้นหากปราศจากนโยบายที่ชัดเจนและมีการควบคุมบังคับใช้ที่ดี บริษัทฯ จะขาดทิศทางในการจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศและอาจสร้างความเสียหายอย่างรุนแรงกับบริษัทฯ

3. วัตถุประสงค์

เพื่อดำเนินการบริหารจัดการความเสี่ยงด้านความปลอดภัยสารสนเทศอย่างเหมาะสมกับธุรกิจของบริษัทฯ ตามแนวทางมาตรฐานสากลในการปกป้องทรัพย์สินสารสนเทศของบริษัทฯ รวมถึงของลูกค้าบุคคลและหน่วยงานภายนอกอื่น ๆ ที่อยู่ในการดูแลรับผิดชอบของบริษัทฯ จากภัยคุกคามต่าง ๆ ทั้งจากภายในและภายนอก ทั้งโดยเจตนาและไม่เจตนาเพื่อให้เป็นไปตามกฎหมายและข้อบังคับต่าง ๆ ที่เกี่ยวข้องอย่างถูกต้อง เช่น

- พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- พรบ. คุ้มครองข้อมูลส่วนบุคคล
- กฎหมายธุรกรรมอิเล็กทรอนิกส์
- กฎหมายลิขสิทธิ์และสิทธิบัตร
- ข้อบังคับจากหน่วยงานของรัฐ
- ภาระผูกพันในสัญญา และความรับผิดชอบต่อลูกค้า บุคคลภายนอกและ หน่วยงานภายนอกที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ

4. ขอบเขตการบังคับใช้นโยบาย

นโยบายความปลอดภัยสารสนเทศฉบับนี้บังคับใช้กับกรรมการ ผู้บริหารและพนักงานของบริษัทฯ เอส โฮเทล แอนด์ รีสอร์ท จำกัด (มหาชน) รวมถึงบริษัทฯ ย่อยและบริษัทฯ ร่วมของบริษัทฯ หากไม่มีนโยบายเรื่องนี้ที่กำหนดเป็นอย่างอื่น

5. บทบาท

บริษัทฯ กำหนดโครงสร้างการกำกับดูแลให้การดำเนินงานเป็นไปโดยสอดคล้องกับนโยบายนี้ ดังนี้

หน่วยงาน/บุคคลากรผู้ปฏิบัติหน้าที่	หน้าที่ และความรับผิดชอบ
ผู้ใช้ทุกคน	ผู้ใช้ทุกคนที่อยู่ภายใต้การบังคับใช้ของนโยบาย ต้องปฏิบัติตามนโยบายฯและมาตรการต่าง ๆ ของบริษัทฯ นอกจากนี้ผู้ใช้ต้องรายงานเหตุการณ์สิ่งผิดปกติ จุดอ่อนและช่องโหว่ต่าง ๆ ที่พบเกี่ยวกับความปลอดภัยสารสนเทศ ให้กับแผนก IT
ผู้บังคับบัญชา	• ผลักดัน สนับสนุนและทบทวนการปฏิบัติงานและมาตรการต่าง ๆ ในขอบเขตความรับผิดชอบให้สอดคล้องกับกฎหมาย ข้อบังคับ และนโยบายบริษัทฯ • สื่อสารนโยบายและมาตรการต่าง ๆ ให้กับพนักงานและบุคคลภายใต้ขอบเขตความรับผิดชอบ • ดำเนินการให้พนักงานทุกคนในสังกัดได้รับการอบรมและมีความตระหนัก ด้านความปลอดภัยสารสนเทศอย่างเพียงพอที่จะรู้เท่าทันภัยและช่องโหว่ ต่าง ๆ ในการปฏิบัติงานและการใช้งานระบบสารสนเทศ
เจ้าของระบบ/ข้อมูลทางธุรกิจ	ทุกระบบ ข้อมูลสารสนเทศ หรือทรัพย์สินประเภทอื่น ๆ ต้องมีเจ้าของที่รับผิดชอบชัดเจน โดยเจ้าของต้อง • ประเมินความเสี่ยงและผลกระทบทางธุรกิจของระบบและข้อมูลสารสนเทศ • อนุมัติยอมรับความเสี่ยงที่เหลือจำกใช้มาตรการ • แบ่งระดับชั้นความปลอดภัยข้อมูล และสิทธิ์การใช้งานในระบบตามตำแหน่งงานหรือหน้าที่การปฏิบัติงานสำหรับข้อมูลสารสนเทศในความรับผิดชอบ • ดำเนินการให้มั่นใจว่าระบบและข้อมูลในความรับผิดชอบได้รับการปกป้องตามความต้องกำรที่กำหนด • ทบทวนประสิทธิผลของมาตรการที่จัดทำไป • กำหนดความต้องการสำหรับระบบและข้อมูลเพื่อความต่อเนื่องทางธุรกิจ เช่น การสำรองและการกู้คืนระบบ
ผู้ควบคุมข้อมูลส่วนบุคคล	ข้อมูลส่วนบุคคลที่ได้รับ จัดเก็บ ประมวลผล ส่งต่อ และทำลาย ต้องมีผู้ควบคุมข้อมูลที่รับผิดชอบชัดเจน โดยผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่ควบคุมการบริหารจัดการข้อมูลส่วนบุคคลให้เป็นไปตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลและนโยบายความปลอดภัยสารสนเทศนี้

แผนก IT	• สนับสนุนงานปฏิบัติการระบบให้กับเจ้าของระบบ / ข้อมูล • ให้คำแนะนำทางเทคนิคกับเจ้าของระบบ / ข้อมูลในการกำหนดความต้องการและเลือกมาตรการการควบคุมที่เหมาะสม • จัดทำรายงานและให้ข้อมูลทางเทคนิคเกี่ยวกับภัยช่องโหว่และมาตรการต่าง ๆ

6. นโยบายความปลอดภัยสารสนเทศ

• ทรัพย์สินข้อมูลสารสนเทศต้องถูกปกป้องตามระดับความปลอดภัยที่กำหนด โดยให้เข้าถึงได้เฉพาะเท่าที่จำเป็นในการดำเนินธุรกิจ หรือบทบังคับทางกฎหมาย

• หน่วยงานต้องดำเนินกิจกรรมกับระบบและข้อมูลสารสนเทศทุกรูปแบบ โดยยึดหลักตาม “มาตรฐานความปลอดภัยสารสนเทศ” ของบริษัทฯ เป็นอย่างน้อย

• พนักงานทุกคนต้องปฏิบัติตามกฎหมายและข้อบังคับต่าง ๆ ที่เกี่ยวข้อง รวมถึงนโยบายของบริษัทฯ อย่างเคร่งครัด

• พนักงานทุกคนต้องรับผิดชอบในการดำเนินกิจกรรมกับข้อมูลสารสนเทศเพื่อธุรกิจของบริษัทฯ เท่านั้นภายในขอบเขตความรับผิดชอบของตน

• ผู้บังคับบัญชาต้องดำเนินการให้มั่นใจได้ว่ามาตรการต่าง ๆ ที่ถูกจัดทำขึ้นต้องสอดคล้องกับนโยบายความปลอดภัยสารสนเทศของบริษัทฯ

• มีการสื่อสาร เพื่อให้มีความรู้ความเข้าใจถึงนโยบายและระเบียบปฏิบัติด้านความปลอดภัยสารสนเทศของบริษัทฯ แก่พนักงานและบุคคลภายนอกที่เกี่ยวข้อง

• ข้อมูลสารสนเทศและระบบต่าง ๆ ต้องถูกกำหนดเจ้าของและความรับผิดชอบที่ชัดเจน

• ระบบต่าง ๆ ต้องได้รับการออกแบบให้มีการควบคุม หรือป้องกันข้อมูลสารสนเทศตามที่กฎหมายกำหนด

• ต้องมีการตรวจสอบการปฏิบัติงานและระบบเพื่อความสอดคล้องกับนโยบายและบทบังคับต่าง ๆ โดยผู้ตรวจสอบประเมินอิสระที่ได้รับอนุญาตจากบริษัทฯ

นโยบายดังกล่าวถือเป็นส่วนหนึ่งของแนวปฏิบัติในการดำเนินงานของบริษัทฯ (Code of Conduct) เพื่อ ความสอดคล้องกับกฎหมายและความรับผิดชอบของบริษัทฯ ที่มีต่อพนักงานและลูกค้า

7. การทบทวนและดูแลนโยบายฯ

นโยบาย ระเบียบ และข้อปฏิบัติต่าง ๆ ต้องถูกทบทวนอย่างสม่ำเสมอ อย่างน้อยปี ละ 1 ครั้งหรือ เมื่อมี การเปลี่ยนแปลงหรือเหตุการณ์สำคัญ เช่น บทบังคับใหม่ตามกฎหมาย พบจุดอ่อนที่สำคัญนโยบายและมาตรฐานอยู่ภายใต้ การควบคุมเอกสาร (document control) ซึ่งต้องถูกจัดเก็บอย่างปลอดภัยตามมาตรฐานของบริษัทฯ

8. การละเมิดฝ่าฝืน

การไม่ปฏิบัติตามนโยบายความปลอดภัยสารสนเทศบริษัทฯ มีสิทธิในการพิจารณาลงโทษตามข้อบังคับเกี่ยวกับการทำงานของบริษัทฯ

ประกาศ ณ วันที่ 24 กุมภาพันธ์ 2566 เป็นต้นไป

- นายอภิศักดิ์ ตันติวรวงศ์ -

(นาย อภิศักดิ์ ตันติวรวงศ์)

ประธานกรรมการ

บริษัท เอส โฮเทล แอนด์ รีสอร์ท จำกัด (มหาชน)