นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒

๑) นโยบายด้านโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ

กำหนดให้มีโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศที่ชัดเจนทั้งในระดับบริหารงานและระดับการปฏิบัติงาน

๒) นโยบายด้านการสร้างความมั่นคงปลอดภัยสารสนเทศด้านบุคลากร

ให้บุคลากรของบริษัทฯ มีความตระหนักรู้เท่าทันภัยคุกคามด้านสารสนเทศ รับทราบและปฏิบัติหน้าที่ความรับผิดชอบของตนเองด้านความมั่นคงปลอดภัย สารสนเทศสม่ำเสมอ

๓) นโยบายด้านการบริหารจัดการทรัพย์สินสารสนเทศ

มีการบริหารการจัดการทรัพย์สินสารสนเทศอย่างมีประสิทธิภาพและกำหนดแนวทางการป้องกันความเสี่ยงต่อทรัพย์สินเหล่านั้นอย่างเหมาะสม

๔) นโยบายด้านการควบคุมการเข้าถึง

มีการควบคุมการเข้าถึงระบบสารสนเทศที่สอดคล้องกับข้อกำหนดทางธุรกิจเพื่อป้องกันการใช้งานระบบสารสนเทศจากผู้ไม่ได้รับอนุญาต

๕) นโยบายด้านการเข้ารหัสข้อมูล

มีการป้องกันข้อมูลที่มีชั้นความลับได้อย่างเหมาะสม โดยใช้เทคโนโลยีการเข้ารหัสข้อมูลที่เป็นมาตรฐานสากล

๖) นโยบายด้านการสร้างความมั่นคงปลอดภัยด้านกายภาพและสิ่งแวดล้อม

มีการกำหนดบริเวณพื้นที่การใช้งานระบบสารสนเทศและอุปกรณ์สารสนเทศ และกำหนดแนวทางป้องกันการเข้าถึงพื้นที่ใช้งานอย่างเหมาะสม

๗) นโยบายด้านความมั่นคงปลอดภัยสำหรับการดำเนินงาน

มีการกำหนดขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบอย่างเป็นลายลักษณ์อักษร มีการสำรองข้อมูล และการตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๘) นโยบายด้านความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

มีการป้องกันข้อมูลที่สื่อสารผ่านช่องทางต่าง ๆ อย่างเหมาะสม

๙) นโยบายด้านการจัดหา การพัฒนา และการบำรุงรักษาระบบ

มีการกำหนดความต้องการพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ และเป็นข้อกำหนดสำคัญในการจัดหา การพัฒนา และการบำรุงรักษาระบบ สารสนเทศของบริษัทฯ

๑๐) นโยบายด้านการควบคุมความมั่นคงปลอดภัยของผู้ให้บริการภายนอก

มีการกำกับ ดูแลและควบคุมผู้ให้บริการจากภายนอกที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศของบริษัทฯ ในการเข้าถึงสารสนเทศที่ไม่ได้รับอนุญาต

๑๑) นโยบายด้านการบริหารจัดการสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศ

มีการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศได้อย่างทันท่วงที

๑๒) นโยบายด้านการบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

มีระบบปฏิบัติงานสำรองของระบบสารสนเทศที่สำคัญ และแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน เพื่อให้พร้อมรองรับการให้บริการระบบสารสนเทศเมื่อเกิดสภาวะวิกฤต

๑๓) นโยบายด้านการปฏิบัติตามข้อกำหนด

ให้มีการปฏิบัติที่สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ และกฎหมายที่เกี่ยวข้อง