นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์

บทนำ

บริษัทได้มีการประมวลผลข้อมูลดิจิทัลและใช้เทคโนโลยีสารสนเทศในการดำเนินงานอย่างมีนัยสำคัญ ดังนั้น สิ่งสำคัญคือ ต้องประเมินและลดความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบงาน (Application) และเทคโนโลยีสารสนเทศ และจำเป็นต้องมีการควบคุม ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) เพื่อปกป้องค์กรจากภัยคุกคามใด ๆ ที่อาจส่งผลกระทบต่อการ ดำเนินธุรกิจและให้บริการลูกค้า นอกจากนี้บริษัทจำเป็นต้องจัดการกับภัยคุกคามความปลอดภัยทางไซเบอร์ที่เกิดขึ้นใหม่ เช่น แรนซัมแวร์ (Ransomware) และการโจมตีด้วยมัลแวร์ (Malware) ความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience) หมายถึงความสามารถ ของบริษัทในการส่งมอบผลิตภัณฑ์และบริการที่ตั้งใจไว้อย่างต่อเนื่องแม้จะเกิดการโจมตีทางไซเบอร์ก็ตาม

หลักการปฏิบัติ

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ และไซเบอร์ของบริษัท มีหลักการปฏิบัติและการควบคุมที่สำคัญ เพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

- ความลับของข้อมูล (Confidentiality) การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึง การใช้งาน และการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลของลูกค้า หรือข้อมูลทางธุรกิจของบริษัท
- ความถูกต้องสมบูรณ์ (Integrity) การทำให้มั่นใจว่าข้อมูลส่วนบุคคลของลูกค้า หรือข้อมูลทางธุรกิจของบริษัทต้องไม่มี การแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- ความพร้อมใช้งาน (Availability) การทำให้มั่นใจว่าลูกค้า และผู้ใช้งานที่ได้รับอนุญาต จะสามารถเข้าถึงข้อมูลและ บริการได้อย่างรวดเร็ว เชื่อถือได้ในเวลาที่ต้องการใช้งาน

ข้อกำหนดด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและไซเบอร์

เพื่อให้สอดคล้องกับข้อกำหนดด้านกฎหมาย บริษัทฯ มีนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ ซึ่งครอบคลุมหัวข้อที่สำคัญดังต่อไปนี้

- การบริหารจัดการทรัพย์สินสารสนเทศ
- การรักษาความปลอดภัยของข้อมูล
- การรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานและระบบเครือข่ายสื่อสารของบริษัท
- การติดตามและเฝ้าระวังเหตุการณ์ด้านความปลอดภัย
- วงจรชีวิตการพัฒนาระบบ
- การจัดการการเข้าถึงระบบสารสนเทศ

- การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
- การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
- การบริหารความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ
- การใช้งานที่ยอมรับได้ (Acceptable Use) ของข้อมูลและระบบงาน
- ความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์
- การใช้ปัญญาประดิษฐ์ (Artificial Intelligence - AI) และการเรียนรู้ของเครื่อง (Machine Learning – ML)

การดำเนินงานที่สำคัญในช่วงปีที่ผ่านมา

- บริษัทจัดให้มีการติดตาม เฝ้าระวัง และมีการรายงานสถานะความเสี่ยงด้านเทคโนโลยีสารสนเทศเทียบกับระดับ ความเสี่ยงที่ยอมรับได้ต่อคณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการกำกับความเสี่ยงอย่างสม่ำเสมอ เพื่อสามารถตัดสินใจและดำเนินนโยบายที่สำคัญในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างทันท่วงที
- บริษัทมอบหมายให้ ฝ่ายเทคโนโลยีสารสนเทศ และฝ่ายความปลอดภัยข้อมูลสารสนเทศและไซเบอร์ มีหน้าที่ดำเนินการเพื่อจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้ การดำเนินการเหล่านี้จะถูกบันทึกลงในระบบติดตามซึ่งใช้สำหรับการติดตามการดำเนินการและการติดตามผลแผนปฏิบัติการดังกล่าวมีการหารือในการประชุมคณะกรรมการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Steering Committee)
- บริษัทจัดให้มีการทดสอบความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์เช่น อีเมลฟิชชิ่ง (Phishing) แก่ผู้บริหารและ พนักงานทุกระดับอย่างสม่ำเสมอ รวมถึงการอบรมเพิ่มเติมเป็นกรณีพิเศษสำหรับพนักงานกลุ่มเสี่ยงด้วย
- บริษัทจัดให้มีการสื่อสารข่าวสารความรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ผ่านช่องทางการสื่อสารภายในอย่างต่อเนื่อง เพื่อให้พนักงานรู้เท่าทันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่