นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์

บทนำ

บริษัทได้มีการประมวลผลข้อมูลดิจิทัลและใช้เทคโนโลยีสารสนเทศในการดำเนินงานอย่างมีนัยสำคัญ ดังนั้น สิ่งสำคัญคือต้องประเมินและลดความเสี่ยงที่เกี่ยวข้องกับการใช้ระบบงาน (Application) และเทคโนโลยีสารสนเทศ และจำเป็นต้องมีการควบคุมความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) เพื่อปกป้ององค์กรจากภัยคุกคามใด ๆ ที่อาจส่งผลกระทบต่อการดำเนินธุรกิจ และให้บริการลูกค้า

นอกจากนี้ บริษัทจำเป็นต้องจัดการกับภัยคุกคามความปลอดภัยทางไซเบอร์ที่เกิดขึ้นใหม่ เช่น แรนซัมแวร์ (Ransomware) และการโจมตีด้วยมัลแวร์ (Malware) ความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience) หมายถึงความสามารถของบริษัทในการส่งมอบผลิตภัณฑ์และบริการที่ตั้งใจไว้อย่างต่อเนื่อง แม้จะเกิดการโจมตีทางไซเบอร์ก็ตาม

หลักการปฏิบัติ

หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ และไซเบอร์ของบริษัท มีหลักการปฏิบัติและการควบคุมที่สำคัญ เพื่อให้บรรลุผลตามวัตถุประสงค์ดังต่อไปนี้

- ความลับของข้อมูล (Confidentiality) – การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึง การใช้งาน และการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลของลูกค้า หรือข้อมูลทางธุรกิจของบริษัท
- ความถูกต้องสมบูรณ์ (Integrity) – การทำให้มั่นใจว่าข้อมูลส่วนบุคคลของลูกค้า หรือข้อมูลทางธุรกิจของบริษัท ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- ความพร้อมใช้งาน (Availability) – การทำให้มั่นใจว่าลูกค้า และผู้ใช้งานที่ได้รับอนุญาต จะสามารถเข้าถึงข้อมูล และบริการได้อย่างรวดเร็ว เชื่อถือได้ ในเวลาที่ต้องการใช้งาน

ข้อกำหนดด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และไซเบอร์

เพื่อให้สอดคล้องกับข้อกำหนดด้านกฎหมาย บริษัทได้จัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ ซึ่งกำหนดบทบาทหน้าที่ของผู้ที่มีส่วนเกี่ยวข้อง และหัวข้อการควบคุมที่จำเป็นดังต่อไปนี้

- บทบาทหน้าที่ของคณะกรรมการบริษัท คณะกรรมการชุดย่อยที่เกี่ยวข้อง ผู้บริหารระดับสูง และหน่วยงานต่าง ๆ (Roles and Responsibility)
- การบริหารจัดการทรัพย์สินสารสนเทศ (IT Asset Management)
- การรักษาความปลอดภัยของข้อมูล (Data Protection)

บริษัท ไทยกรุ๊ป โฮลดิ้งส์ จำกัด (มหาชน) 315 อาคารไทยกรุ๊ป ชั้น 12 ถนนสีลม แขวงสีลม เขตบางรัก กรุงเทพมหานคร 10500
Thai Group Holdings Public Company Limited 315 Thai Group Bldg., 12 Fl., Silom Rd., Silom, Bangrak, Bangkok 10500
T: 0 2632 1224 www.tgh.co.th
ทะเบียนเลขที่ / เลขประจำตัวผู้เสียภาษีอากร Registration No. / Tax ID No. 0107561000285

- การรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานและระบบเครือข่ายสื่อสารของบริษัท (Platform and Network Security)
- การติดตามและเฝ้าระวังเหตุการณ์ด้านความปลอดภัย (Security Monitoring)
- วงจรชีวิตการพัฒนาระบบ (Software Development Life Cycle – SDLC)
- การจัดการการเข้าถึงระบบสารสนเทศ (IT Identity and Access Management)
- การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security)
- การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security) ครอบคลุมถึงกระบวนการบริหารจัดการการเปลี่ยนแปลง การบริหารจัดการเหตุการณ์ผิดปกติและปัญหา การบริหารจัดการขีดความสามารถของระบบ และการบริหารจัดการเครื่องคอมพิวเตอร์
- การบริหารความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ (IT Continuity management) ครอบคลุมถึงแผนการกู้คืนระบบสารสนเทศ (IT Disaster Recovery Plan – IT DRP) และแผนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan – CIRP)
- การใช้งานที่ยอมรับได้ (Acceptable Use) ของข้อมูลและระบบงาน
- ความพร้อมด้านการรับมือภัยคุกคามทางไซเบอร์ (Cyber Resilience)

ทั้งนี้ ฝ่ายบริหารความเสี่ยงและการกำกับดูแล จัดให้มีการสื่อสารนโยบายไปยังผู้บริหาร และพนักงานทุกระดับในหลายช่องทาง อาทิเช่น ระบบเครือข่ายภายใน (Intranet) อีเมลประชาสัมพันธ์ และการอบรมพนักงานใหม่ เป็นต้น

การดำเนินงานที่สำคัญในช่วงปีที่ผ่านมา

- บริษัทจัดให้มีการติดตาม เฝ้าระวัง และมีการรายงานสถานะความเสี่ยงด้านเทคโนโลยีสารสนเทศเทียบกับระดับความเสี่ยงที่ยอมรับได้ ต่อคณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการกำกับความเสี่ยงอย่างสม่ำเสมอ เพื่อสามารถตัดสินใจ และดำเนินนโยบายที่สำคัญในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศได้อย่างทันท่วงที
- บริษัทมอบหมายให้ฝ่ายบริหารธุรกิจ สายงานเทคโนโลยีสารสนเทศ และฝ่ายความปลอดภัยเทคโนโลยีสารสนเทศ มีหน้าที่ดำเนินการเพื่อจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้อยู่ภายในระดับความเสี่ยงที่ยอมรับได้ การดำเนินการเหล่านี้จะถูกบันทึกลงในระบบติดตามซึ่งใช้สำหรับการติดตามการดำเนินการและการติดตามผล แผนปฏิบัติการดังกล่าวมีการหารือในการประชุมคณะกรรมการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Steering Committee)
- บริษัทจัดให้มีการทดสอบความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์ เช่น อีเมลฟิชชิ่ง (Phishing) แก่ผู้บริหาร และพนักงานทุกระดับอย่างสม่ำเสมอ รวมถึงการอบรมเพิ่มเติมเป็นกรณีพิเศษสำหรับพนักงานกลุ่มเสี่ยงด้วย
- บริษัทจัดให้มีการสื่อสารข่าวสารความรู้เกี่ยวกับความปลอดภัยทางไซเบอร์ ผ่านช่องทางการสื่อสารภายในอย่างต่อเนื่อง เพื่อให้พนักงานรู้เท่าทันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใหม่

บริษัท ไทยกรุ๊ป โฮลดิ้งส์ จำกัด (มหาชน) 315 อาคารไทยกรุ๊ป ชั้น 12 ถนนสีลม แขวงสีลม เขตบางรัก กรุงเทพมหานคร 10500
Thai Group Holdings Public Company Limited 315 Thai Group Bldg., 12 Fl., Silom Rd., Silom, Bangrak, Bangkok 10500
T: 0 2632 1224 www.tgh.co.th
ทะเบียนเลขที่ / เลขประจำตัวผู้เสียภาษีอากร Registration No. / Tax ID No. 0107561000285