นโยบายการกำกับดูแลความมั่นคงปลอดภัย ระบบสารสนเทศ

บริษัท เงินเทอร์โบ จำกัด (มหาชน) (“บริษัท”) ตระหนักดีว่า เทคโนโลยีสารสนเทศและระบบเครือข่ายเป็นกลไกสำคัญในการขับเคลื่อนธุรกิจการให้บริการทางการเงินที่มีประสิทธิภาพและยั่งยืน อย่างไรก็ตาม การเติบโตของเทคโนโลยีย่อมมาพร้อมกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งอาจส่งผลกระทบต่อความต่อเนื่องทางธุรกิจ ความน่าเชื่อถือของบริษัท ตลอดจนความปลอดภัยของข้อมูลส่วนบุคคลของลูกค้าและผู้มีส่วนได้เสีย

คณะกรรมการบริษัทจึงได้จัดทำ “นโยบายการกำกับดูแลความมั่นคงปลอดภัยระบบสารสนเทศ” ฉบับนี้ขึ้น โดยอ้างอิงและประยุกต์ใช้แนวทางมาตรฐานสากล เช่น ISO/IEC 27001 และกรอบความมั่นคงปลอดภัยไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา (NIST Cybersecurity Framework) เพื่อเป็นกรอบแนวทางปฏิบัติในการปกป้อง ดูแล และจัดการความปลอดภัยของโครงสร้างพื้นฐานสารสนเทศของบริษัทอย่างเป็นระบบและยั่งยืน

1. ขอบเขตการบังคับใช้

- กรรมการ ผู้บริหาร พนักงาน ลูกจ้างชั่วคราว และพนักงานสัญญาจ้างทุกคนของบริษัท และบริษัทย่อยในเครือทั้งหมด
- ระบบสารสนเทศ อุปกรณ์คอมพิวเตอร์ ระบบเครือข่ายข้อมูล ซอฟต์แวร์ และโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศทั้งหมดของบริษัท
- ผู้ให้บริการภายนอก (Outsource) ที่ปรึกษา คู่ค้า และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึง สัมผัส หรือใช้งานระบบสารสนเทศและข้อมูลของบริษัท

2. โครงสร้างการกำกับดูแลและความรับผิดชอบ

เพื่อให้ระบบการกำกับดูแลมีความรัดกุมและเป็นไปตามหลักการกำกับดูแลกิจการที่ดี (CG) บริษัทกำหนดโครงสร้างความรับผิดชอบไว้ดังนี้:

- **คณะกรรมการบริษัท (Board of Directors):** มีหน้าที่อนุมัตินโยบายนี้ กำกับดูแลให้บริษัทมีโครงสร้างการจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสมเพียงพอ และสนับสนุนการส่งเสริมความรู้ อบรมเพิ่มพูนทักษะด้านเทคโนโลยีสารสนเทศและภัยคุกคามทางไซเบอร์แก่กรรมการบริษัทและผู้บริหารระดับสูงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าคณะกรรมการมีขีดความสามารถในการกำกับดูแล (Tone at the Top) อย่างแท้จริง
- **คณะกรรมการบริหารความเสี่ยง (Risk Management Committee):** มีหน้าที่ประเมินความเสี่ยง ติดตามรายงานสถานะความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ (IT & Cyber Risk Register) และพิจารณาความพร้อมของแผนรองรับการดำเนินธุรกิจอย่างต่อ

เนื่อง (IT BCP/DRP) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์สำคัญเกิดขึ้น

- **คณะกรรมการตรวจสอบ (Audit Committee):** มีหน้าที่กำกับดูแลและติดตามผลการตรวจสอบระบบเทคโนโลยีสารสนเทศ (IT Audit) โดยหน่วยงานตรวจสอบภายในหรือผู้เชี่ยวชาญอิสระภายนอก เพื่อให้มั่นใจว่าการควบคุมภายในด้านไอทีมีประสิทธิภาพ โปร่งใส และสอดคล้องกับกฎหมายที่เกี่ยวข้อง
- **ผู้บริหารสูงสุดฝ่ายเทคโนโลยีสารสนเทศ (CTO หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย):** มีหน้าที่นำนโยบายไปปฏิบัติ จัดทำแนวปฏิบัติย่อย ควบคุมดูแลความปลอดภัยในการใช้งานระบบ ตลอดจนรายงานสถานะระบบและเหตุการณ์ภัยคุกคามรวมถึงแนวทางป้องกันต่อคณะกรรมการบริหารความเสี่ยงเป็นประจำอย่างน้อยปีละ 1 ครั้ง

3. การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล

บริษัทกำหนดให้มีการประยุกต์ใช้และปฏิบัติตามหลักเกณฑ์มาตรฐานความมั่นคงปลอดภัยสารสนเทศขั้นพื้นฐาน 5 ด้าน (Identify, Protect, Detect, Respond, Recover) ดังต่อไปนี้:

3.1. การระบุตัวตนและประเมินความเสี่ยง (Identify)

- จัดทำทะเบียนสินทรัพย์สารสนเทศ (IT Asset Inventory) และทำการจำแนกประเภทข้อมูลความลับ (Data Classification) ตามระดับความสำคัญของข้อมูลอย่างชัดเจน
- จัดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์เป็นประจำทุกปี เพื่อวิเคราะห์จุดอ่อนและระบุมาตรการควบคุมที่เหมาะสม

3.2. การป้องกันระบบและสิทธิ์การเข้าถึง (Protect)

- **การควบคุมการเข้าถึงระบบ (Access Control):** ปฏิบัติตามหลักการกำหนดสิทธิ์เท่าที่จำเป็นเพื่อปฏิบัติงานเท่านั้น (Least Privilege / Need-to-Know Basis) และกำหนดให้มีการทบทวนสิทธิ์การเข้าถึงของพนักงานเป็นประจำอย่างน้อยทุก 12 เดือน หรือทันทีเมื่อมีการเปลี่ยนแปลงหน้าที่หรือพ้นสภาพการเป็นพนักงาน
- **ระบบพิสูจน์ตัวตนที่มั่นคงปลอดภัย:** บังคับให้ใช้การระบุตัวตนแบบหลายปัจจัย (Multi-Factor Authentication - MFA) สำหรับการเข้าถึงระบบที่สำคัญหรือการทำงานจากภายนอกสำนักงาน (Remote Access / VPN)
- **การรักษาความปลอดภัยเครือข่าย:** จัดตั้งระบบป้องกันระบบเครือข่าย เช่น ไฟร์วอลล์ (Firewall) ระบบตรวจจับการบุกรุก (IDS/IPS) และระบบซอฟต์แวร์ป้องกันมัลแวร์ที่เป็นมาตรฐานสากลบนอุปกรณ์คอมพิวเตอร์ทั้งหมด

3.3. การตรวจจับภัยคุกคาม (Detect)

- จัดให้มีระบบการติดตาม ตรวจสอบ และเก็บบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Log Management) ให้เป็นไปตามกฎหมายที่เกี่ยวข้อง เพื่อให้สามารถตรวจพบความผิดปกติบนระบบสารสนเทศได้อย่างทันท่วงที
- ดำเนินการทดสอบเพื่อค้นหาช่องโหว่ (Vulnerability Assessment) และการทดสอบเจาะระบบ (Penetration Testing) ของระบบงานที่สำคัญโดยผู้เชี่ยวชาญอิสระจากภายนอก

3.4. การตอบสนองต่อเหตุการณ์ผิดปกติ (Respond & Board Escalation SLA)

- จัดตั้งแผนรับมือภัยคุกคามไซเบอร์และเหตุการณ์ผิดปกติ (Cybersecurity Incident Response Plan) ที่มีกระบวนการและขั้นตอนการปฏิบัติงานที่ชัดเจน เพื่อควบคุมและจำกัดขอบเขตความเสียหายของระบบงานและข้อมูล
- **การรายงานเหตุภัยคุกคามรุนแรงสูงสุด (Critical Incident Reporting SLA):** ในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์หรือมีข้อมูลลูกค้ารั่วไหลในระดับรุนแรง (Critical Incident) ที่มีนัยสำคัญต่อชื่อเสียง การเงิน หรือการดำเนินงานของบริษัท ฝ่ายจัดการมีหน้าที่ต้องรายงานเหตุการณ์ดังกล่าวต่อคณะกรรมการบริหารความเสี่ยงและคณะกรรมการบริษัทรับทราบ ภายใน 24 ชั่วโมง นับแต่ที่ได้ตรวจพบหรือได้รับการยืนยันเหตุการณ์

3.5. การกู้คืนระบบ และความต่อเนื่องทางธุรกิจ (Recover)

- จัดให้มีระบบการสำรองข้อมูล (Data Backup) และจัดเก็บข้อมูลสำรองไว้ภายนอกพื้นที่ปฏิบัติงานหลัก (Off-site Backup) หรือบนระบบคลาวด์ที่มีความมั่นคงปลอดภัยสูง และทำการทดสอบกู้คืนข้อมูลเป็นประจำอย่างสม่ำเสมอ
- จัดทำและฝึกซ้อมแผนรองรับการดำเนินธุรกิจต่อเนื่องด้านเทคโนโลยีสารสนเทศ (IT Disaster Recovery Plan - IT DRP) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าระบบเทคโนโลยีสารสนเทศที่สำคัญสามารถฟื้นคืนกลับมาใช้งานได้ตามระยะเวลาที่กำหนด (RTO/RPO Targets) หากเกิดภัยพิบัติหรือระบบล่ม

4. การรักษาความตระหนักรู้และการอบรมด้านไซเบอร์

- พนักงานและผู้บริหารทุกคนของบริษัท ต้องเข้ารับการอบรมความรู้ความเข้าใจด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Awareness Training) เป็นประจำทุกปี เพื่อ

ปรับปรุงความตระหนักรู้ต่อกลลวงสมัยใหม่ (เช่น Phishing, Social Engineering)

- บริษัทจัดให้มีการทดสอบจำลองเหตุการณ์ส่งอีเมลลวง (Phishing Simulation) แก่พนักงาน เพื่อเสริมสร้างความพร้อมและลดความเสี่ยงจากการถูกโจมตีทางเทคนิค
- จัดให้มีช่องทางการรายงานสิ่งผิดปกติหรือจุดอ่อนระบบที่พนักงานพบเจอได้อย่างปลอดภัย และสนับสนุนให้พนักงานรายงานความเสี่ยงโดยไม่มีผลกระทบในเชิงลบต่อหน้าที่การงาน หรือบทลงโทษทางวินัย (No-Retaliation for Vulnerability Reporting)

5. การรักษาความปลอดภัยด้านการเชื่อมต่อและข้อมูลของบุคคลภายนอก

- ในการทำสัญญากับผู้ให้บริการภายนอก (Outsource) หรือคู่ค้าที่จำเป็นต้องสัมผัสระบบหรือข้อมูลของบริษัท บริษัทต้องจัดให้มีการลงนามในข้อตกลงรักษาความลับ (Non-Disclosure Agreement - NDA) และแนบเงื่อนไขความมั่นคงปลอดภัยสารสนเทศเป็นส่วนหนึ่งของสัญญาเสมอ
- บริษัทจะดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอก (Vendor Security Assessment) ก่อนการจัดซื้อจัดจ้าง และทำการทบทวนสิทธิ์การเข้าถึงของผู้ให้บริการดังกล่าวทันทีเมื่อเสร็จสิ้นภารกิจงาน

6. การบูรณาการร่วมกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)

การออกแบบ ปรับปรุง และควบคุมความปลอดภัยของระบบสารสนเทศทั้งหมดของบริษัท ต้องสอดคล้องและสนับสนุนมาตรการรักษาความมั่นคงปลอดภัยขั้นต่ำตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) กำหนดอย่างเคร่งครัด เพื่อป้องกันมิให้ข้อมูลของลูกค้าและพนักงานเกิดการรั่วไหล สูญหาย หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต ตลอดจนช่วยปกป้องสิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Rights) ของลูกค้าอย่างสมบูรณ์แบบ

7. บทลงโทษกรณีฝ่าฝืนนโยบาย

การฝ่าฝืน ไม่ปฏิบัติตาม หรือกระทำการใดๆ ที่จงใจให้ระบบเทคโนโลยีสารสนเทศของบริษัทเสื่อมเสีย ตกอยู่ในความเสี่ยง หรือก่อให้เกิดความเสียหายร้ายแรงต่อระบบความปลอดภัย ถือเป็นการกระทำความผิดวินัยพนักงานอย่างร้ายแรง และจะได้รับการพิจารณาโทษตามข้อบังคับเกี่ยวกับการทำงานของบริษัท ตั้งแต่การตักเตือน การพักงาน จนถึงการเลิกจ้างโดยไม่ได้รับค่าชดเชย ตลอดจนการดำเนินคดีแพ่ง คดีอาญา และคดีตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จนถึงที่สุด

8. การทบทวนและประเมินผลนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและไซเบอร์ฉบับนี้ จะได้รับการทบทวนและประเมินความเพียงพอเหมาะสมจากคณะกรรมการบริหารความเสี่ยงและคณะกรรมการบริษัทเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือทันทีที่มีการเปลี่ยนแปลงทางกฎหมาย มาตรฐานสากล หรือการเปลี่ยนแปลงเทคโนโลยีและโมเดลธุรกิจที่มีนัยสำคัญ เพื่อให้สอดคล้องและทันสมัยอยู่เสมอ