นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัท ไทยคม จำกัด (มหาชน)

24 พฤษภาคม 2564

Thaicom Public Company Limited
(Company Registration No. 0107536000897)
63/21, Rattanatibet Road
Nonthaburi 11000, Thailand.
www.thaicom.net, www.ipstar.com
Tel. (66 2) 596 5060
Fax. (66 2) 591 0705

บริษัท ไทยคม จำกัด (มหาชน)

นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

กลุ่มบริษัท ไทยคม จำกัด (มหาชน) ("บริษัท") ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศต่อการดำเนินธุรกิจของบริษัท จึงได้จัดทำนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อป้องกันภัยหรือลดความเสี่ยงจากการคุกคาม อันอาจก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อธุรกิจของบริษัท โดยอ้างอิงตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรฐานหรือแนวปฏิบัติในระดับสากล

ขอบเขต

นโยบายฉบับนี้ครอบคลุมการป้องกันภัยคุกคาม และการรักษาความมั่นคงปลอดภัยไซเบอร์ของระบบเทคโนโลยีสารสนเทศของบริษัท ทั้งที่อยู่ภายในหรือภายนอกสถานที่ปฏิบัติงานของบริษัท รวมทั้งระบบคลาวด์ที่บริษัทจัดหาหรือใช้บริการ ซึ่งครอบคลุมถึงการใช้งานโดยผู้ใช้ในระบบจากทุกหน่วยงานของบริษัท และบริษัทในเครือที่บริษัทมีอำนาจควบคุม

หลักการและแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์

บริษัทใช้หลักการ "Zero Trust" ที่มีสมมุติฐานว่า ภัยคุกคามทางไซเบอร์เป็นสิ่งที่เกิดขึ้นได้ทุกเวลาและไม่สามารถหลีกเลี่ยงได้ ดังนั้นจึงต้องมีการลดความเสี่ยงและผลกระทบ โดยการจำกัดการเข้าถึงระบบและทรัพยากรต่างๆ เท่าที่จำเป็นเท่านั้น และจำเป็นต้องมีการดูแลเฝ้าระวัง เพื่อตรวจหาการใช้งานที่ไม่ปกติและน่าสงสัยว่าเป็นอันตรายอยู่ตลอดเวลาสม่ำเสมอ

โครงสร้างการทำงานและหน้าที่ความรับผิดชอบ

บริษัทแต่งตั้งคณะกรรมการเพื่อกำกับดูแลเทคโนโลยีสารสนเทศ ซึ่งประกอบด้วยหัวหน้างานระดับสูงสุดของสายงานที่สำคัญ โดยมีประธานเจ้าหน้าที่บริหารเป็นประธาน และหัวหน้างานด้านเทคโนโลยีสารสนเทศเป็นเลขานุการ โดยทำหน้าที่กำกับดูแลการดำเนินการด้านเทคโนโลยีสารสนเทศของบริษัทให้มีประสิทธิผลสูงสุด ควบคู่กับการบริหารจัดการความเสี่ยงและผลกระทบจากภัยคุกคามทางไซเบอร์ และกลยุทธ์ของบริษัท

Thaicom Public Company Limited
(Company Registration No. 0107536000897)
63/21, Rattanatibet Road
Nonthaburi 11000, Thailand.
www.thaicom.net, www.ipstar.com
Tel. (66 2) 596 5060
Fax. (66 2) 591 0705

หน้าที่	ความรับผิดชอบ
ประธานเจ้าหน้าที่บริหาร (CEO)	กำหนดกลยุทธในภาพรวม ติดตามกำกับดูแลการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัท และอนุมัติแนวปฏิบัติต่างๆ ด้านระบบสารสนเทศ
หัวหน้าส่วนงานเทคโนโลยีสารสนเทศ	ออกแบบพัฒนานโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้มีความปลอดภัยและเกิดประโยชน์สูงสุดต่อบริษัท
หัวหน้างานหรือผู้บังคับบัญชาทุกระดับ	ชี้แจงให้พนักงานทราบถึงนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ รวมทั้งดูแล แนะนำ และตักเตือนหรือรายงานกรณีที่พบเห็นการปฏิบัติที่ไม่ถูกต้องหรือไม่เหมาะสม
พนักงานทุกคน	เรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศโดยเคร่งครัด และให้ความร่วมมือกับบริษัทอย่างเต็มที่ในการสอดส่องการใช้งานที่ไม่ปกติและอาจมีอันตราย โดยแจ้งให้บริษัททราบทันทีเมื่อพบเห็น
พนักงานที่มีหน้าที่เกี่ยวข้องกับบุคคลภายนอก	จัดให้มีการควบคุมดูแลบุคคลภายนอกให้ปฏิบัติตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศโดยเคร่งครัด
หน่วยงานตรวจสอบภายใน	กำหนดให้มีการตรวจสอบการบริหารจัดการ การดำเนินงาน และการปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศตามความจำเป็น

นโยบาย

บริษัทต้องมีการกำหนดนโยบายและแนวปฏิบัติที่ต้องเป็นไปตามกฎหมายและตามหลักการและวัตถุประสงค์ ดังต่อไปนี้

1. สิทธิและการควบคุมการเข้าถึงระบบและทรัพยากรต่าง ๆ

การกำหนดการให้สิทธิการเข้าถึงระบบและทรัพยากรต่างๆ จะให้เท่าที่จำเป็นตามหน้าที่ความรับผิดชอบเท่านั้น โดยต้องมีระบบจัดการการควบคุมการเข้าถึงสถานที่ ระบบ อุปกรณ์ ข้อมูล และทรัพยากรต่างๆ ที่ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตอย่างเคร่งครัด โดยมีขอบเขตแนวทางอย่างน้อยดังต่อไปนี้

1) จัดทำบัญชีทรัพย์สินและความเป็นเจ้าของ (Asset Inventory and Ownership)
2) การควบคุมการเข้าถึงระบบและข้อมูลเฉพาะผู้ที่ได้รับอนุญาต โดยใช้ปัจจัยหลายๆ อย่างในการตรวจสอบและยืนยันตัวบุคคล (Multi-Factor Authentication)
3) มาตรฐานการเข้ารหัสและการบริหารกุญแจ (Cryptography and Key Management)
4) ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

Thaicom Public Company Limited
(Company Registration No. 0107536000897)
63/21, Rattanatibet Road
Nonthaburi 11000, Thailand.
www.thaicom.net, www.ipstar.com
Tel. (66 2) 596 5060
Fax. (66 2) 591 0705

2. การบริหารจัดการดูแลเฝ้าระวังการเพื่อตรวจหาการใช้งานที่ผิดปกติและอาจเป็นอันตราย

การบริหารจัดการระบบและการเฝ้าระวังการใช้งานเพื่อตรวจหาการใช้งานที่ผิดปกติและอาจเป็นอันตราย ต้องทำอย่างสม่ำเสมอและทั่วถึงเคร่งครัด โดยมีขอบเขตแนวทางอย่างน้อยดังต่อไปนี้

1) การพิจารณาทบทวน Account and Privilege และความเสี่ยงที่เกี่ยวข้องเจ้าของ (Account and Privilege Defense)
2) การออกแบบเครือข่ายที่มีการแบ่งขอบเขตและจำกัดการ และมีการควบคุมดูแลเฝ้าระวังในระดับ application และการใช้งาน (Network Zoning, Micro-segmentation of the Application layer and Application-aware Firewall)
3) การบริหารจัดการความปลอดภัยสำหรับเครือข่าย (Network Security Management) โดยการตรวจหาการเข้าถึงโดยผิดปกติและอาจจะมีอันตราย (Hunt for Network Intrusions)
4) การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)
5) การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ (Systems Acquisition, Development and Maintenance) ต้องคำนึงถึงความปลอดภัยเป็นหลักรวมถึงต้องมีการบริหารช่องโหว่ (Vulnerability Management) อย่างเหมาะสม

3. การบริหารจัดการความต่อเนื่องของธุรกิจ

การบริหารจัดการความต่อเนื่องของธุรกิจต้องมีการพิจารณาและเตรียมแผนรองรับสำหรับกรณีการจู่โจมทางไซเบอร์ (Cyber Attacks) และมีการทบทวนการปฏิบัติให้สอดคล้องกับกฎหมายและข้อบังคับที่เกี่ยวข้องอย่างสม่ำเสมอ (Regulatory and Compliance)

4. การทบทวนและเปลี่ยนแปลงนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

บริษัทอาจทำการปรับปรุงหรือแก้ไขนโยบายนี้เป็นครั้งคราวเพื่อให้สอดคล้องกับข้อกำหนดตามกฎหมาย การเปลี่ยนแปลงการดำเนินงานของบริษัท รวมถึงข้อเสนอแนะและความคิดเห็นจากหน่วยงานต่างๆ โดยบริษัทจะแจ้งการเปลี่ยนแปลงให้ทราบอย่างชัดเจนผ่านการประกาศที่เหมาะสมของบริษัท

ประกาศ ณ วันที่ 24 พฤษภาคม พ.ศ. 2564

(นาย ประเสริฐ บุญสัมพันธ์)
ประธานคณะกรรมการบริษัท
บริษัท ไทยคม จำกัด (มหาชน)

Thaicom Public Company Limited
(Company Registration No. 0107536000897)
63/21, Rattanatibet Road
Nonthaburi 11000, Thailand.
www.thaicom.net, www.ipstar.com
Tel. (66 2) 596 5060
Fax. (66 2) 591 0705