



THAI EASTERN BIO POWER

นโยบายด้านเทคโนโลยีสารสนเทศ

บริษัท ไทยอีสเทิร์น ไบโอ พาวเวอร์ จำกัด

ฉบับที่ 18 (สิงหาคม 2567)

ประกาศ ที่ TEBP-BOD 018
เรื่อง นโยบายด้านเทคโนโลยีสารสนเทศ

1. บทนำ

บริษัท ไทยอีสเทิร์น ไบโอ พาวเวอร์ จำกัด (“บริษัท”) และบริษัทย่อย มีทรัพย์สินสารสนเทศเพื่อสนับสนุนประสิทธิภาพการดำเนินงานให้สามารถตอบสนองเป้าหมายทางธุรกิจ ดังนั้นจึงถือว่าทรัพย์สินสารสนเทศเป็นทรัพย์สินที่สำคัญ ผู้ปฏิบัติงานจะต้องใช้และดูแลรักษาให้อยู่ในสภาพที่พร้อมใช้งานได้อย่างมีประสิทธิภาพอยู่ตลอดเวลา ด้วยเหตุนี้ บริษัท จึงได้ประกาศนโยบายเพื่อกำหนดให้มีมาตรฐาน แนวปฏิบัติ และขั้นตอนการปฏิบัติงาน ให้ครอบคลุมการบริหารจัดการทรัพย์สินสารสนเทศ และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อเป็นแนวทางในการใช้งานที่เหมาะสมสอดคล้องกับนโยบายระบบบริหารจัดการของบริษัท

2. หลักการและเหตุผล

บริษัทกำหนดให้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้โดยสร้างความร่วมมือจากทุกฝ่าย ให้มีความรู้ ความเข้าใจในทรัพย์สินสารสนเทศ เพื่อทำให้เกิดประสิทธิภาพสูงสุด

นโยบายด้านสารสนเทศฉบับนี้ได้ถูกจัดทำขึ้นมา เพื่อ

1. ให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยสามารถดำเนินงานได้อย่างต่อเนื่อง
2. บริหารความเสี่ยง และกำหนดแนวทางป้องกันปัญหาที่เกิดขึ้นจากการใช้งานอุปกรณ์เครื่องมือเทคโนโลยีสารสนเทศอย่างถูกต้อง และป้องกันภัยคุกคามต่าง ๆ
3. ให้สอดคล้องกับหลักการกำกับดูแลกิจการที่ดี และข้อกำหนดทางกฎหมาย ระเบียบปฏิบัติที่เกี่ยวข้อง จรรยาบรรณทางธุรกิจและนโยบายระบบบริหารจัดการของบริษัทฯ

โดยกำหนดให้มีการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบันอย่างน้อยปีละครั้ง รวมถึงต้องมีการประเมินความเสี่ยงอย่างน้อยปีละครั้ง ซึ่งต้องมีการระบุความเสี่ยงที่เกี่ยวข้อง จัดลำดับความสำคัญของข้อมูลและระบบคอมพิวเตอร์ กำหนดระดับความเสี่ยงที่ยอมรับได้ และกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยง

ขอบเขต

นโยบายนี้มีผลบังคับใช้กับพนักงานทุกฝ่าย ทุกแผนก ทุกระดับชั้นและตำแหน่งโดยไม่มีการยกเว้น ทั้งนี้รวมถึงบุคคลอื่นๆ ที่ได้รับอนุญาตให้ใช้ระบบเครือข่าย คอมพิวเตอร์ แม้าข่าย ระบบคอมพิวเตอร์ เครื่อง

คอมพิวเตอร์ คอมพิวเตอร์แบบพกพา อุปกรณ์สื่อสารแบบพกพา หรือ อุปกรณ์สื่อสารโทรคมนาคมเพื่อการเข้าถึงสารสนเทศของบริษัท

บทบาทและความรับผิดชอบ

คณะกรรมการบริษัท

- ทบทวนและอนุมัตินโยบาย

คณะกรรมการบริหาร

- กำหนดทิศทางของนโยบาย และทบทวนนโยบายด้านความปลอดภัยสารสนเทศ
- ตัดสินใจในการติดต่อกับหน่วยงานบังคับใช้กฎหมาย รวมถึงข้อยกเว้นและการเปลี่ยนแปลงที่อาจจะเกิดขึ้น

ฝ่ายบริหารทรัพยากรบุคคล

- แจกหรือส่งมอบคู่มือและนโยบายสารสนเทศแก่พนักงานที่เข้าใหม่

ผู้ใช้งาน

- ทำความเข้าใจนโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงานด้านความปลอดภัยสารสนเทศตาม

นโยบายของบริษัท

- ใช้ทรัพย์สินของบริษัทอย่างมีจริยธรรม และถูกต้องตามกฎหมาย
- เมื่อมีเหตุการณ์ที่อาจจะส่งผลกระทบต่อความปลอดภัยสารสนเทศแจ้งให้กับหัวหน้างาน หรือผู้บริหารด้านความปลอดภัยสารสนเทศให้ทราบทันที

3. นโยบายและมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

- 3.1 กำหนดให้พื้นที่ระบบคอมพิวเตอร์แม่ข่าย (Server) ของบริษัทเป็นพื้นที่หวงห้าม เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ห้ามผู้ที่มิได้รับอนุญาตเข้าพื้นที่โดยพลการ
- 3.2 กำหนดให้มีการบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network) มีการแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน มีป้องกันผู้บุกรุก
- 3.3 กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก การตรวจสอบบันทึกการปฏิบัติงาน วิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกต่างๆ ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น
- 3.4 เฉพาะผู้ที่ได้รับสิทธิ์จึงจะสามารถเข้าถึงข้อมูลและระบบเครือข่ายได้ตามสิทธิ์ที่ได้รับมอบหมาย โดยห้ามมิ ใหบุคคลที่ไม่มีอำนาจเกี่ยวข้อง เข้าถึง (Access Risk) แก้ไขเปลี่ยนแปลง (Integrity Risk)

หรือ ก่อให้เกิดความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์และเครือข่าย (Availability Risk) โดยเด็ดขาด

- 3.5 การเข้าสู่ระบบจากระยะไกล (Remote Access) ผู้ระบบเครือข่ายคอมพิวเตอร์ของบริษัท สามารถทำได้บนพื้นฐานของความจำเป็นเท่านั้นและจะต้องได้รับการอนุมัติจาก Chief Financial Officer ก่อน และต้องมีการควบคุมการเข้าสู่ระบบอย่างรัดกุม โดยให้สื่อสารได้เฉพาะกับ VPN (Virtual Private Network)
- 3.6 บุคคลภายนอกที่ต้องการสิทธิ์ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท จะต้องลงนามในสัญญาไม่เปิดเผยข้อมูลของบริษัทก่อน และต้องได้รับการอนุมัติอย่างเป็นทางการ ลายลักษณ์อักษรจากผู้จัดการแผนกไอที จึงจะสามารถขอเปิดสิทธิ์ให้เข้าสู่ระบบได้
- 3.7 กำหนดให้มีการควบคุมการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการรายอื่น (IT Outsourcing)
- 3.8 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์พกพา (Notebook) และ mobile devices
 - 3.8.1 ห้ามพนักงานใช้คอมพิวเตอร์บริษัทเพื่อประโยชน์ส่วนตัวไม่ว่าจะเป็นในหรือนอกเวลาปฏิบัติงาน
 - 3.8.2 ให้ผู้ใช้งานเก็บรักษา Username และ Password ของตนอย่างเป็นความลับ ห้ามมิให้เผยแพร่ หรือเปิดเผย และต้องมีการเปลี่ยนรหัสผ่านเมื่อระบบแจ้งเตือนทุกครั้ง
 - 3.8.3 ห้ามไม่ให้ผู้อื่นใช้บัญชีของตน และหากเกิดปัญหาจากการให้ใช้บัญชี เช่นการละเมิด ลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย หรือกระทำการใดๆ ที่ไม่เหมาะสม เจ้าของบัญชีต้องเป็นผู้รับผิดชอบ เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำ
 - 3.8.4 ให้ผู้ใช้งานออกจากระบบทุกครั้งที่ไม่ได้ใช้งาน หรือเมื่อไม่อยู่ประจำหน้าเครื่อง
 - 3.8.5 ห้ามเชื่อมต่อ Website ที่ไม่เกี่ยวข้องกับธุรกิจของบริษัท เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคม และให้ระมัดระวังไม่ให้เข้า website ที่อาจมีความเสี่ยงทำให้ระบบสารสนเทศของบริษัท ติดไวรัส
 - 3.8.6 การเก็บข้อมูล ให้เก็บในเครื่องแม่ข่าย (Server) ไม่ให้บันทึกข้อมูลไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ใช้งานอยู่ และผู้ใช้งานพึงลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องแม่ข่าย เพื่อเป็นการประหยัดพื้นที่จัดเก็บข้อมูล
 - 3.8.7 ห้ามมิให้พนักงานติดตั้ง โปรแกรมคอมพิวเตอร์ หรืออุปกรณ์ต่อพ่วงอื่นใด นอกเหนือจากที่บริษัทได้จัดไว้ให้ กรณีมีความจำเป็นต้องติดตั้ง โปรแกรมคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วง

- เพิ่มเติม ให้แจ้งผู้ดูแลระบบเป็นผู้ดำเนินการให้ โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของบริษัท ต้องเป็น โปรแกรมที่บริษัทได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายเท่านั้น
- 3.8.8 ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของบริษัท
- 3.8.9 ห้ามใช้คอมพิวเตอร์และระบบเครือข่ายของบริษัทในการให้ร้าย หรือส่งต่อข้อมูลที่อาจเป็นการละเมิดผู้อื่น อันอาจทำให้ผู้อื่นเสื่อมเสียและเกิดความเดือดร้อน
- 3.8.10 ห้ามใช้บัญชีอีเมลของบริษัทฯ เพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย พรบ. ขัดก้าหนด หรือนโยบายต่าง ๆ ที่บริษัทฯ ได้ประกาศไว้และพนักงานพึงใช้ข้อความสุภาพ หรือใช้ข้อความที่สุภาพชนทั่วไปพึงใช้ในข้อความที่ส่งไปถึงบุคคลอื่น
- 3.8.11 ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมลที่มีเนื้อหาหรือรูปภาพที่ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง ข่มขู่ ลามกอนาจาร การข่มขู่,ทางเพศหรืออีเมลที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรมหรือศาสนา รวมถึงอีเมลที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อบริษัทฯ
- 3.8.12 ก่อนเปิดไฟล์ที่เป็น executable file เช่น .exe .com ต้องใช้โปรแกรมป้องกันไวรัสตรวจสอบก่อนเปิดไฟล์
- 3.8.13 เพื่อความปลอดภัยในการใช้ระบบเครือข่ายคอมพิวเตอร์ กรณีผู้ใช้งานพบไวรัสคอมพิวเตอร์จะต้องแจ้งให้ผู้ดูแลระบบดำเนินการกำจัดไวรัสโดยเร็ว
- 3.9 หน้าที่ของผู้ดูแลระบบ
- 3.9.1 ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องต่อเชื่อมผ่าน Firewall หรือระบบรักษาความปลอดภัยอื่น ๆ
- 3.9.2 ให้ติดตั้งระบบป้องกัน Malicious software รวมถึงการปรับปรุง Security Patch อยู่เสมอ
- 3.9.3 ต้องสำรองข้อมูลระบบงาน อย่างสม่ำเสมอ และควรจัดเก็บอย่างน้อย 2 สถานที่ เพื่อประโยชน์ในการกู้คืนข้อมูลเมื่อมีปัญหาเกิดขึ้น
- 3.9.4 ผู้ดูแลระบบต้องทดสอบข้อมูลสำรองว่าพร้อมนำกลับมาใช้งานกรณีที่เกิดเหตุการณ์ฉุกเฉิน และมีการซักซ้อม ทุก 3 เดือน เพื่อให้เกิดผลกระทบต่อการดำเนินงานและการบริการของบริษัทน้อยที่สุด
- 3.9.5 การเปิดเผยข้อมูลบริษัททางอินเทอร์เน็ต จะต้องพิจารณาถึงผลกระทบ และภาพลักษณ์ที่ดีขององค์กร และต้องได้รับอนุมัติจาก Chief Strategy Officer (CSO)

- 3.9.6 เมื่อผู้ใช้งานระบบลาออกจากบริษัท หรือเปลี่ยนแปลงเงื่อนไขการเข้าถึงระบบ ผู้ดูแลระบบจะต้องทำการถอดถอนหรือปรับปรุงสิทธิ์ให้ถูกต้องไม่เกิน 1 วันทำการ
- 3.9.7 ต้องทดสอบความพร้อมใช้งานของระบบสารสนเทศ ระบบเครือข่ายสำรอง อย่างน้อยปีละ 3 ครั้ง
- 3.9.8 ผู้ดูแลระบบต้องจัดทำแผนแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ (IT Contingency Plan) และให้มีการทบทวน และทดสอบแผนอย่างน้อยปีละ 1 ครั้ง
- 3.9.9 ผู้ดูแลระบบจะต้องควบคุมการเข้า-ออกพื้นที่ระบบคอมพิวเตอร์แม่ข่าย (Server Room/Data Center) และต้องจัดบันทึกการขออนุมัติเข้า-ออก ของบุคคลภายนอกเป็นหลักฐาน พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย 1 ปี
- 3.9.10 ผู้ดูแลระบบต้องไม่ใช้อำนาจหน้าที่ของตนไปในการเข้าถึงข้อมูลที่ได้รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น และต้องไม่เปิดเผยข้อมูลที่ตนได้รับมาจากหรือเนื่องจากการปฏิบัติหน้าที่ผู้ดูแลเครือข่ายคอมพิวเตอร์ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่ควรเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ

ทั้งนี้ผู้ใช้งานต้องปฏิบัติตามนโยบายการใช้งานระบบสารสนเทศฉบับนี้ รวมถึงข้อกำหนดกฎหมาย ด้านคอมพิวเตอร์ที่ได้ประกาศใช้ในประเทศไทย ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ รวมทั้งกฎระเบียบและนโยบายของบริษัทอย่างเคร่งครัด และหากผู้ใช้งานกระทำผิด ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

3.10. การพิจารณาบทลงโทษทางวินัยกับผู้ฝ่าฝืนไม่ปฏิบัติตามนโยบายด้านเทคโนโลยีสารสนเทศ

หากพบว่ามีผู้ฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายด้านเทคโนโลยีสารสนเทศ ฉบับนี้ บริษัทจะดำเนินการสอบสวนเพื่อหาข้อเท็จจริง โดยให้คณะกรรมการสอบสวนที่แต่งตั้งโดยคณะกรรมการบริหารเป็นผู้มีอำนาจในการสอบสวน และกำหนดแนวทางการลงโทษทางวินัยรวมถึงโทษอื่นๆ ตามกฎหมายที่เกี่ยวข้อง

เพื่อให้นโยบายด้านเทคโนโลยีสารสนเทศฉบับนี้มีความเหมาะสม และสอดคล้องกับสถานการณ์สภาพของธุรกิจ หรือกฎระเบียบที่มีการเปลี่ยนแปลง จึงกำหนดให้มีการทบทวนนโยบายฉบับนี้เป็นประจำทุกปี

นโยบายฉบับนี้ให้มีผลใช้บังคับตั้งแต่วันที่ 7 สิงหาคม 2567 เป็นต้นไป

ประกาศ ณ วันที่ 7 สิงหาคม 2567
บริษัท ไทยอีสเทิร์น ไบโอ พาวเวอร์ จำกัด



(นายเฉลิม โกกนุทาภรณ์)

ประธานคณะกรรมการ