Company Policy

เรื่อง : นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ

หมายเลขเอกสาร : PB-CO-25

	ชื่อ-สกุล	ตำแหน่ง	ลายมือชื่อ	วัน/เดือน/ปี
จัดทำโดย	น.ส.รัชนีวรรณ ดีเดช	ผู้ช่วยผู้จัดการฝ่ายทรัพยากรบุคคล		25/02/2568
ทบทวนโดย	นายสุทธิเกียรติ กิตติภัทรากุล	ประธานเจ้าหน้าที่บริหาร		25/02/2568
อนุมัติโดย	นายคุณา วิทยฐานกรณ์	ประธานกรรมการบริษัท		25/02/2568

ประวัติการแก้ไข

ครั้งที่แก้ไข	อ้างอิง DAR เลขที่	วันที่มีผลบังคับใช้	รายละเอียดของการแก้ไข
00	-	31/01/2566	จัดทำและประกาศใช้ครั้งแรก
01	-	29/02/2567	ทบทวนประจำปี ไม่มีการเปลี่ยนแปลงเนื้อหา
02	-	01/10/2567	(1) แก้ไขชื่อบริษัทโดยเพิ่มคำว่า "(มหาชน)" ต่อท้ายชื่อบริษัท (2) แก้ไขโลโก้บริษัทให้มีคำว่า "(มหาชน)"
03	-	25/02/2568	(1) เพิ่มเติมวัตถุประสงค์ของนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (2) เพิ่มเติมเนื้อหาข้อ 3.3 เรื่อง การป้องกันการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศ (3) แก้ไขหมายเลขเอกสารจาก PB-CO-32 เป็น PB-CO-25 (4) แก้ไขโลโก้บริษัทให้เป็นแบบใหม่

1. บทนำ

บริษัท ยืมมั้ย (ประเทศไทย) จำกัด (มหาชน) ("บริษัท") ให้ความสำคัญต่อการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ ซึ่งถือเป็นปัจจัยสำคัญที่ช่วยส่งเสริมการดำเนินธุรกิจและเพิ่มประสิทธิภาพการทำงาน ซึ่งหากบริษัทมีการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศที่ไม่เพียงพอและเหมาะสมอาจก่อให้เกิดความเสียหายต่อบริษัทและผู้ใช้งาน ดังนั้น บริษัทจึงได้กำหนดนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศขึ้น เพื่อใช้เป็นแนวทางให้พนักงานของบริษัททั้งองค์กรมีหน้าที่ปฏิบัติตามนโยบายฉบับนี้

2. วัตถุประสงค์

2.1 เพื่อกำหนดแนวทางให้กรรมการ ผู้บริหาร พนักงาน และผู้เกี่ยวข้อง สามารถใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศของบริษัทให้เป็นไปตามวัตถุประสงค์และเป้าหมายในการดำเนินธุรกิจเท่านั้น

2.2 เพื่อป้องกันและลดความเสี่ยงจากการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศของบริษัท ไปในทางมิชอบด้วยกฎหมาย หรือกฎระเบียบของหน่วยงานต่างๆ ที่เกี่ยวข้อง ซึ่งอาจก่อให้เกิดความเสียหายต่อบริษัท

2.3 เพื่อกำหนดมาตรการสำรองข้อมูลและสารสนเทศของบริษัท เพื่อรักษาความปลอดภัยของข้อมูลในกรณีที่เกิดภัยคุกคามต่อระบบคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ให้สามารถดำเนินงานได้อย่างต่อเนื่อง

3. นโยบาย

3.1. การกำหนดแนวปฏิบัติในการให้บริการด้านเทคโนโลยีสารสนเทศ (Information Technology Service Policy)

บริษัทกำหนดระเบียบบริษัท และระเบียบปฏิบัติ ที่เกี่ยวข้องในการบริหารทรัพยากรด้านเทคโนโลยีสารสนเทศเพื่อให้สามารถสนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศของบริษัท ให้สอดคล้องกับแผนกลยุทธ์บริษัท ได้อย่างเพียงพอและเหมาะสม รวมถึงแนวปฏิบัติและเกณฑ์ในการให้บริการด้านเทคโนโลยีสารสนเทศ เพื่อให้การบริการมีความต่อเนื่อง และช่วยสนับสนุนการดำเนินงานของบริษัทได้อย่างเต็มประสิทธิภาพ

3.2. การตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Assessment Policy)

บริษัทกำหนดให้มีกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยให้ครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยง และการควบคุมความเสี่ยงให้อยู่ในเกณฑ์ที่บริษัทยอมรับได้ รวมถึงจัดให้มีผู้รับผิดชอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

3.3. การป้องกันการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศ

เพื่อเป็นการป้องกันการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศของบริษัทไม่ให้ใช้งานในทางมิชอบ บริษัทจึงกำหนดหลักการเพื่อเป็นแนวปฏิบัติให้แก่กรรมการ ผู้บริหาร พนักงาน และผู้เกี่ยวข้อง ถือปฏิบัติดังนี้

(1) กรรมการ ผู้บริหาร พนักงาน และผู้เกี่ยวข้อง พึงใช้งานคอมพิวเตอร์และเทคโนโลยีสารสนเทศของบริษัทให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายอื่นที่เกี่ยวข้อง

(2) คอมพิวเตอร์และเทคโนโลยีสารสนเทศรวมถึงอุปกรณ์ต่อพ่วงที่ใช้สำหรับการปฏิบัติงานถือเป็นทรัพย์สินของบริษัท ผู้บริหารและพนักงานพึงใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศรวมถึงอุปกรณ์ต่อพ่วง เพื่องานของบริษัทเท่านั้น ตลอดถึงดูแล บำรุง รักษาให้ปลอดภัย และพร้อมใช้งาน

(3) ห้ามมีการเปลี่ยนแปลง ทำซ้ำ ลบทิ้ง หรือทำลายข้อมูลของบริษัท รวมถึงห้ามเปิดเผยข้อมูลที่อยู่ในระบบข้อมูลของบริษัท โดยไม่ได้รับอนุญาตจากผู้มีอำนาจของบริษัท

(4) กรรมการ ผู้บริหาร พนักงาน และผู้เกี่ยวข้อง พึงปกป้องดูแลรักษาบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ห้ามใช้ร่วมกับผู้อื่น ห้ามการเผยแพร่ แจกจ่าย หรือทำให้ผู้อื่นล่วงรู้

(5) ห้ามกรรมการ ผู้บริหาร พนักงาน และผู้เกี่ยวข้อง ใช้อีเมลของบริษัท ในการส่งข้อความหรือรูปภาพที่ให้ร้าย ทำให้เสื่อมเสีย หรือหยาบคาย ลามก ข่มขู่ ก่อกวน สร้างความรำคาญให้กับผู้อื่น หรือขัดต่อกฎหมาย วัฒนธรรม ประเพณี ศีลธรรมอันดีงาม

3.4. การจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Policy)

บริษัทกำหนดให้มีระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และดำเนินการประกาศแนวปฏิบัติดังกล่าวให้ผู้เกี่ยวข้องรับทราบ โดยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องครอบคลุม 10 ข้อ ได้แก่

หมวดที่ 1 การควบคุมอุปกรณ์สารสนเทศส่วนตัวและการใช้งาน VPN

เพื่อกำหนดแนวทางปฏิบัติสำหรับการควบคุมการใช้งานอุปกรณ์พกพา หรืออุปกรณ์สารสนเทศส่วนตัวในพื้นที่ปฏิบัติงานซึ่งต้องมีการมาตรการด้านความปลอดภัยกำกับ รวมถึงการทำงานทางไกลโดยการรีโมท ก็จำเป็นต้องมีการควบคุมเพื่อให้สามารถปฏิบัติงานได้อย่างปลอดภัยเช่นกัน

หมวดที่ 2 ความมั่นคงปลอดภัยที่เกี่ยวกับการจัดสรรทรัพย์สินสารสนเทศสำหรับบุคลากร

เพื่อให้บริษัทสามารถจัดสรรทรัพย์สินสารสนเทศสำหรับบุคลากรเมื่อเริ่มต้นเข้าทำงาน และเมื่อยุติการปฏิบัติหน้าที่ได้อย่างเหมาะสม

หมวดที่ 3 การบริหารจัดการทรัพย์สิน

ทรัพย์สิน หมายถึง ทรัพย์สินที่เกี่ยวข้องกับข้อมูล เช่น ข้อมูล ซอฟต์แวร์ หรืออุปกรณ์ที่เกี่ยวข้องในการประมวลผล นอกจากนี้บริษัทควรกำหนดให้มีเจ้าของทรัพย์สินเพื่อรับผิดชอบทรัพย์สินนั้น โดยที่เจ้าของทรัพย์สินอาจมอบหมายให้ผู้อื่นดูแลและควบคุมทรัพย์สินแทน แต่อย่างไรก็ตามเจ้าของทรัพย์สินยังคงเป็นผู้ที่รับผิดชอบสูงสุดในทรัพย์สินดังกล่าว เพื่อให้มีการระบุทรัพย์สินของบริษัท และกำหนดหน้าที่ความรับผิดชอบในการป้องกันทรัพย์สินอย่างเหมาะสม

หมวดที่ 4 การควบคุมการเข้าถึง (Access Control Policy)

เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย และเพื่อลดความเสี่ยงด้านการเข้าใช้งานอย่างไม่เหมาะสม จำเป็นต้องควบคุมการเข้าใช้ระบบสารสนเทศ โดยพิจารณาถึงความเหมาะสมในการเข้าใช้งานระบบจากความจำเป็น และความต้องการทางธุรกิจ

หมวดที่ 5 การเข้ารหัสข้อมูล

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และเพื่อป้องกันความลับ การปลอมแปลงหรือความถูกต้องของสารสนเทศ

หมวดที่ 6 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environment Security)

เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพ ที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นสินทรัพย์ของบริษัท

หมวดที่ 7 ความมั่นคงปลอดภัยสำหรับการดำเนินการ

เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

หมวดที่ 8 ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของบริษัท

หมวดที่ 9 การจัดหา พัฒนา และดูแลระบบสารสนเทศ

เพื่อให้แน่ใจว่ามีการสร้างความปลอดภัยสารสนเทศให้กับระบบสารสนเทศ ตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านความปลอดภัยสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ

หมวดที่ 10 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของบริษัทได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม และเพื่อให้มีวิธีการที่สอดคล้องกันและได้ผลสำหรับการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

3.5. การบริหารจัดการสารสนเทศเพื่อสร้างความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP)

เพื่อป้องกันการหยุดชะงักในการดำเนินงานของบริษัท ที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ ไม่ว่าจะด้วยอุบัติเหตุ ภัยธรรมชาติ หรือจากเหตุการณ์ที่ไม่สามารถคาดการณ์ได้ล่วงหน้า ซึ่งก่อให้เกิดความเสียหายต่อบริษัทไม่มากก็น้อย ดังนั้น บริษัทจึงกำหนดให้มีการจัดทำระเบียบบริษัท เรื่อง แผนบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ เพื่อลดความรุนแรงของผลกระทบจากเหตุการณ์ดังกล่าวให้อยู่ในระดับที่ยอมรับได้ และให้สามารถดำเนินธุรกิจหลักของบริษัทต่อไปได้

3.6. กำหนดให้บุคลากรภายใต้บริษัท ปฏิบัติตามนโยบาย ระเบียบบริษัท และระเบียบปฏิบัติ เกี่ยวกับด้านเทคโนโลยีสารสนเทศของบริษัทอย่างเคร่งครัด ผู้ฝ่าฝืนมีความผิด และต้องได้รับการลงโทษทางวินัยตามที่บริษัทกำหนดไว้

3.7. นโยบายฉบับนี้ถือเป็นแม่บท เพื่อให้พนักงานของบริษัททั้งองค์กรรับทราบถึงการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศของบริษัทเบื้องต้น ทั้งนี้ เพื่อให้ระบบสารสนเทศของบริษัทมีการจัดการอย่างเหมาะสม และมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างถูกต้อง บริษัทยังได้กำหนดระเบียบปฏิบัติในด้านต่างๆ ที่เกี่ยวข้องกับการทำงานของฝ่ายเทคโนโลยีสารสนเทศเพิ่มเติม เพื่อให้ฝ่ายเทคโนโลยีสารสนเทศมีแนวปฏิบัติและขั้นตอนของการปฏิบัติ ในเชิงลึกที่ครอบคลุมและป้องกันภัยคุมคามต่างๆ ด้วย

4. การทบทวนนโยบาย

นโยบายฉบับนี้ กำหนดให้มีการทบทวนเป็นประจำอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีเหตุการณ์เปลี่ยนแปลง