นโยบายเทคโนโลยีสารสนเทศ

บริษัท แอดเทค ฮับ จำกัด (มหาชน) (“**บริษัท**”) คำนึงถึงความสำคัญของการนำเทคโนโลยีสารสนเทศเข้ามาช่วยเพิ่มศักยภาพและประสิทธิภาพในการดำเนินงานของบริษัท เพื่อก่อให้เกิดกระบวนการบริหารจัดการที่เป็นระบบ มีระเบียบเป็นขั้นตอน ลดความซ้ำซ้อน สนองความต้องการของผู้ใช้บริการและช่วยให้การดำเนินธุรกิจมีความต่อเนื่อง

บริษัทจึงเล็งเห็นว่าการนำเทคโนโลยีสารสนเทศเข้ามาใช้ในการดำเนินงาน จำเป็นต้องกำหนดแนวทางการพัฒนาให้สอดคล้องกับกลยุทธ์และวิสัยทัศน์ของบริษัท รวมถึงกฎหมาย ข้อบังคับ มาตรฐานสากลต่าง ๆ ที่เกี่ยวข้องและการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศในปัจจุบัน เพื่อให้การบริหารทางด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ มีประสิทธิผล มีความมั่นคงปลอดภัย และมีกรอบในการบริหารจัดการและแก้ไขปัญหาทางระบบเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน เพื่อใช้เป็นแนวทางในการป้องกันผลกระทบที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ รวมถึงเพื่อให้ผู้ที่เกี่ยวข้องเกิดความเชื่อมั่นในการใช้งานระบบสารสนเทศของบริษัท

วัตถุประสงค์

เพื่อให้บริษัทมีแนวนโยบายในการดำเนินงาน หรือการจัดการทางด้านเทคโนโลยีสารสนเทศและให้ผู้ที่เกี่ยวข้องกับสารสนเทศ ทั้งผู้บริหารและบุคลากรทุกระดับ หน่วยงานภายนอกและบุคคลภายนอกที่เข้ามาเกี่ยวข้องกับสารสนเทศของบริษัทได้มีแผนงานและกรอบการปฏิบัติที่ชัดเจน อันจะนำไปสู่การประสานงานและการดำเนินการที่มีประสิทธิภาพ มีความปลอดภัยในการใช้งานและใช้บริการอย่างสูงสุดและมีมาตรฐานยิ่งขึ้น อีกทั้งกำหนดมาตรการป้องกันที่เหมาะสมเพื่อควบคุมความเสี่ยงและลดความเสียหายต่าง ๆ ที่อาจเกิดขึ้น จากกรณีที่ทรัพย์สินไม่สามารถใช้งานได้ สูญหาย เสียหาย บกพร่องหรือถูกคุกคามด้านความมั่นคงปลอดภัย

กฎหมายและกฎระเบียบต่าง ๆ ที่เกี่ยวข้อง

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 และฉบับที่แก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2558 และ (ฉบับที่ 3) พ.ศ. 2558
- พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2533
- ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศของหน่วยงานรัฐ พ.ศ. 2553 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2556
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย

บทบังคับใช้และบทลงโทษ

นโยบายเทคโนโลยีสารสนเทศฉบับนี้ ให้มีผลบังคับใช้นับจากวันที่ประกาศให้มีผลบังคับใช้ต่อผู้ใช้งานระบบสารสนเทศของบริษัทและบริษัทย่อยทั้งหมดโดยไม่มีการยกเว้น ผู้ฝ่าฝืนจะมีความผิดและต้องได้รับการลงโทษทางวินัยตามระเบียบที่บริษัทกำหนดไว้

การเผยแพร่นโยบาย

ฝ่ายเทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในการประกาศและเผยแพร่นโยบายไปยังผู้ใช้งานระบบสารสนเทศของบริษัท เพื่อช่วยให้เกิดความเข้าใจในบทบาทของตนเองในการใช้งานเทคโนโลยีสารสนเทศและปกป้องทรัพย์สินของบริษัท

การทบทวนนโยบาย

นโยบายเทคโนโลยีสารสนเทศฉบับนี้ต้องได้รับการทบทวน ปรับปรุงให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญของสภาพแวดล้อมต่าง ๆ เช่น สภาพธุรกิจ กฎเกณฑ์ กฎหมายและเทคโนโลยี เป็นต้น โดยถือเป็นหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศในการทบทวนและปรับปรุง โดยมีผู้บริหารฝ่ายเทคโนโลยีสารสนเทศเป็นผู้ควบคุมดูแลให้เกิดการทบทวนและปรับปรุงตามที่ได้กำหนดไว้

นโยบายการบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศ

1. การบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ (Change Management Policy)

เพื่อกำหนดแนวทางการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศ และลดความผิดพลาดในการดำเนินการเปลี่ยนแปลง รวมถึงระบบงานสามารถสนับสนุนธุรกิจของบริษัทได้อย่างต่อเนื่องและมีประสิทธิภาพ

1.1 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการกำหนดประเภทของการเปลี่ยนแปลง (Change Type) เพื่อใช้ในการดำเนินการบันทึก จำแนกประเภท ประเมิน และกำหนดผู้อนุมัติสำหรับคำร้องขอการเปลี่ยนแปลง โดยผู้มีอำนาจอนุมัติให้หมายถึงผู้จัดการฝ่ายขึ้นไปหรือผู้ที่ได้รับมอบหมายให้มีอำนาจอนุมัติ

1.2 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำขั้นตอนปฏิบัติงานสำหรับการบริหารจัดการการเปลี่ยนแปลงระบบสารสนเทศและให้บันทึกการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร

1.3 ผู้ร้องขอและผู้ดำเนินการเปลี่ยนแปลงต้องดำเนินการวิเคราะห์ผลกระทบและความเสี่ยงในการ ดำเนินการเปลี่ยนแปลง เพื่อเตรียมมาตรการรองรับการเปลี่ยนแปลงในแต่ละกิจกรรม

1.4 ผู้ที่ร้องขอให้มีการเปลี่ยนแปลงจะต้องจัดทำแผนงานภาพรวม สำหรับการดำเนินการการเปลี่ยนแปลงโดยกำหนดวันเวลาที่ต้องการดำเนินงานและทรัพยากรที่จำเป็น เป็นต้น และแจ้งให้ผู้ที่เกี่ยวข้องรับทราบถึงแผนการเปลี่ยนแปลง

1.5 ผู้ดำเนินการเปลี่ยนแปลงต้องจัดทำแผนสำหรับย้อนกลับสู่สภาวะเดิม (Fallback Plan) เพื่อใช้สำหรับแก้ไขการเปลี่ยนแปลงเมื่อต้องการให้กลับสู่สภาวะเดิม หากการเปลี่ยนแปลงไม่สามารถทำได้สำเร็จตามวัตถุประสงค์ที่ต้องการ

2. การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)

เพื่อกำหนดแนวทางการบริหารจัดการความต่อเนื่องในการให้บริการระบบสารสนเทศ ในกรณีที่เกิดเหตุฉุกเฉินหรือเหตุการณ์ความมั่นคงปลอดภัยด้านสารสนเทศใด ๆ ซึ่งอาจส่งผลกระทบให้การดำเนินธุรกิจของบริษัทหยุดชะงัก

2.1 บริษัทต้องจัดให้มีศูนย์คอมพิวเตอร์สำรอง และระบบสารสนเทศสำรอง เพื่อรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง และลดผลกระทบเมื่อเกิดเหตุการณ์ที่ส่งผลให้การดำเนินธุรกิจหยุดชะงัก โดยมีผู้บริหารระดับสูงสุดของบริษัทเป็นผู้มีอำนาจตัดสินใจในการสั่งการ

2.2 หน่วยงานผู้ใช้บริการและฝ่ายเทคโนโลยีสารสนเทศต้องร่วมกันกำหนดกรอบมาตรฐาน (Framework) เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจและครอบคลุมข้อกำหนดความมั่นคงปลอดภัยด้านสารสนเทศที่ได้กำหนดไว้ รวมถึงมีความสะดวกในการจัดลำดับความสำคัญของแผนและกิจกรรมที่ต้องดำเนินการ

2.3 หน่วยงานผู้ใช้บริการและฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการประเมินความเสี่ยงและบันทึกความเสี่ยงที่อาจส่งผลให้การให้บริการระบบสารสนเทศขาดความต่อเนื่องและทำข้อตกลงเงื่อนไขความต้องการ ได้แก่ ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD) หรือระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective: RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery point objective: RPO) อย่างเป็นลายลักษณ์อักษร

2.4 หน่วยงานผู้ใช้บริการและฝ่ายเทคโนโลยีสารสนเทศต้องควบคุม กำกับให้มีการจัดทำแผนการบริหารจัดการความต่อเนื่องทางธุรกิจภายใต้กรอบมาตรฐานที่กำหนดไว้และเผยแพร่ให้ผู้ที่เกี่ยวข้องรับทราบ ทั้งนี้ แผนการบริหารจัดการความต่อเนื่องทางธุรกิจควรได้รับการทดสอบอย่างน้อยปีละ 1 ครั้ง

2.5 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำแผนรองรับกรณีเกิดเหตุฉุกเฉิน (Disaster Recovery Plan: DRP) โดยให้มีความสอดคล้องกับแผนการบริหารจัดการความต่อเนื่องทางธุรกิจของบริษัท

2.6 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการสำรองข้อมูล เอกสาร ซอฟต์แวร์ และระบบงาน รวมถึงอุปกรณ์ต่าง ๆ และบุคลากรที่จำเป็น เพื่อสนับสนุนให้การกู้คืนระบบสารสนเทศให้เป็นไปอย่างรวดเร็วที่สุดหลังจากเกิดการหยุดชะงักในการให้บริการหรือเหตุภัยพิบัติ

2.7 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการทดสอบแผนรองรับกรณีเกิดเหตุฉุกเฉิน (Disaster Recovery Plan: DRP) อย่างน้อยปีละ 1 ครั้ง และให้มีการบันทึกผลการทดสอบเพื่อให้มั่นใจได้ว่าธุรกิจสามารถดำเนินต่อไปได้เมื่อเกิดเหตุการณ์ที่กระทบกับกระบวนการทางธุรกิจของบริษัท

3. การบริหารจัดการเหตุขัดข้อง และการบริหารจัดการคำร้องขอ (Incident and Service Request Management Policy)

เพื่อกำหนดแนวทางการแก้ไขเหตุขัดข้อง การจัดหา และการจัดการระบบงานคอมพิวเตอร์ของบริษัทให้สามารถสนับสนุนการให้บริการธุรกิจของบริษัทได้อย่างรวดเร็ว มีความต่อเนื่อง มีความถูกต้องน่าเชื่อถือและมีประสิทธิภาพ

3.1 การบริหารจัดการเหตุขัดข้อง

3.1.1 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการกำหนดเกณฑ์ในการวัดระดับผลกระทบ (Impact) ความเร่งด่วน (Urgency) และลำดับความสำคัญ (Priority) ของเหตุขัดข้อง

3.1.2 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดหน้าที่ความรับผิดชอบในการแก้ไขเหตุขัดข้องพร้อมทั้งจัดทำขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการเหตุขัดข้องและบริหารจัดการคำร้องขอเพื่อใช้เป็นแนวทางในการดำเนินงาน

3.1.3 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการบันทึกรายละเอียดของเหตุขัดข้องและคำร้องขอให้ครบถ้วนตามขั้นตอนปฏิบัติงานที่ระบุไว้ เพื่อใช้เป็นหลักฐานและใช้ประกอบการวิเคราะห์หาวิธีการแก้ไขและรายงานผลการดำเนินงานต่อไป

3.1.4 บุคลากรฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการแก้ไขเหตุขัดข้องและคำร้องขอที่ได้รับแจ้งมาอย่างรวดเร็วเต็มความสามารถให้สอดคล้องกับข้อตกลงการให้บริการที่ได้กำหนดไว้

3.1.5 กรณีที่ผู้รับเรื่องไม่สามารถแก้ไขเหตุขัดข้องและคำร้องขอได้ด้วยตนเองจะต้องยกระดับการให้บริการ (Escalation) ไปยังผู้เกี่ยวข้องตามลำดับ เพื่อเพิ่มประสิทธิภาพและความรวดเร็วในการดำเนินงาน

3.2 การบริหารจัดการคำร้องขอ

3.2.1 การจัดหาระบบงานคอมพิวเตอร์

- หน่วยงานที่ต้องการให้มีการจัดหาระบบงานคอมพิวเตอร์ ต้องระบุความต้องการระบบงานคอมพิวเตอร์ของแต่ละหน่วยงาน รวมทั้งจัดทำเป็นโครงการและขออนุมัติงบประมาณในการจัดทำโครงการ โดยให้มีการบันทึกเป็นลายลักษณ์อักษรและได้รับการอนุมัติจากผู้บริหารระดับฝ่ายและฝ่ายเทคโนโลยีสารสนเทศ
- ฝ่ายเทคโนโลยีสารสนเทศต้องให้การสนับสนุนด้านข้อมูลที่เกี่ยวข้องกับการจัดหาระบบงานคอมพิวเตอร์ เช่น หน่วยงานภายนอก คุณสมบัติของเครื่องคอมพิวเตอร์ ข้อมูลความมั่นคงปลอดภัยด้านสารสนเทศ หรือข้อมูลอื่นใดที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศตามที่ได้รับการร้องขอ

4. การจัดการระดับการให้บริการ (Service Level Management Policy)

เพื่อกำหนดแนวทางในการจัดทำข้อตกลงสำหรับระดับการให้บริการด้านเทคโนโลยีสารสนเทศระหว่างฝ่ายเทคโนโลยีสารสนเทศและผู้ใช้งานระบบสารสนเทศของบริษัทให้อยู่ในเกณฑ์ที่สามารถยอมรับได้

4.1 บริษัทต้องกำหนดให้มีการจัดทำสัญญาที่ระบุถึงข้อตกลงระดับการให้บริการ ดังต่อไปนี้

4.1.1 ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) ระหว่างหน่วยงานผู้ให้บริการ และผู้ใช้งาน

4.1.2 ข้อตกลงการให้บริการระดับปฏิบัติงาน (Operational Level Agreement: OLA) ระหว่างหน่วยงานผู้ให้บริการภายในบริษัท

4.1.3 สัญญาการให้บริการระหว่างหน่วยงานผู้ให้บริการและหน่วยงานภายนอก

4.2 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำข้อตกลงการให้บริการระหว่างฝ่ายเทคโนโลยีสารสนเทศและผู้ใช้งาน ทั้งนี้ ข้อตกลงการให้บริการต้องได้รับการอนุมัติอย่างเป็นทางการจากผู้บริหารระดับฝ่ายเทคโนโลยีสารสนเทศและตัวแทนผู้บริหารจากหน่วยงานต่าง ๆ ภายในบริษัท

4.3 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการบริหารจัดการงานบริการด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับสัญญาข้อตกลงการให้บริการ

4.4 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการตรวจสอบวิเคราะห์ประสิทธิภาพการทำงาน แนวโน้มของการให้บริการเป็นระยะตามความเหมาะสมและนำมาแก้ไขปรับปรุงเพื่อเพิ่มประสิทธิภาพในการดำเนินงานต่อไป

4.5 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำเอกสารหรือรายการการให้บริการ (Service Catalogue) ที่ให้บริการอยู่ในปัจจุบันโดยครอบคลุมทุก ๆ การให้บริการที่อยู่ในข้อตกลงการให้บริการซึ่งได้รับการยอมรับเงื่อนไขการให้บริการจากตัวแทนผู้บริหารของหน่วยงานต่าง ๆ ภายในบริษัท

4.6 การแก้ไขเอกสารใด ๆ ที่เกี่ยวข้องกับความต้องการด้านการให้บริการ (Service Requirement) ระดับการให้บริการ (Service Level Agreement) หรือรายละเอียดการให้บริการ (Service Catalogue) ต้องถูกดำเนินการผ่านการบริหารจัดการการเปลี่ยนแปลง (Change Management) ที่บริษัทกำหนดไว้

5. การจัดการด้านงบประมาณและการควบคุมการใช้จ่ายของการให้บริการ (Budgeting and Accounting for Services Policy)

เพื่อกำหนดแนวทางในการบริหารจัดการงบประมาณและควบคุมค่าใช้จ่ายที่เกี่ยวข้องกับการสนับสนุนการให้บริการด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม

5.1 ฝ่ายเทคโนโลยีสารสนเทศต้องดำเนินการจัดสรรงบประมาณให้ครบถ้วนและเพียงพอต่อการให้บริการและควบคุมการใช้จ่ายงบประมาณให้เกิดประสิทธิภาพสูงสุด

5.2 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดให้มีการจัดสรรงบประมาณและจะต้องพิจารณาต้นทุนทางตรง (Direct Cost) ต้นทุนทางอ้อม (Indirect Cost) ค่าใช้จ่ายของการจัดซื้อทรัพย์สินสารสนเทศ (IT Asset) ค่าใช้จ่ายจากการใช้ทรัพยากรร่วมกัน (Shared Resource Cost) ค่าใช้จ่ายประจำสำนักงาน (General and Administrative Expense) ค่าใช้จ่ายในการจัดจ้างหน่วยงานภายนอก (Externally Supplied Service Cost) ค่าใช้จ่ายของการจัดจ้างบุคลากร (People) ค่าใช้จ่ายของการทำประกัน (Insurance Expense) และค่าใช้จ่ายด้านลิขสิทธิ์ต่าง ๆ (License Expense) รวมถึงค่าใช้จ่ายอื่น ๆ ที่เกี่ยวข้องในการให้บริการ

5.3 ฝ่ายเทคโนโลยีสารสนเทศต้องติดตามการใช้งบประมาณและตรวจสอบงบประมาณคงเหลือเพื่อให้บริหารการใช้งบประมาณได้อย่างมีประสิทธิภาพ

6. การบริหารข้อมูลสารสนเทศเพื่อรายงานผลการให้บริการ (Service Reporting Policy)

เพื่อให้บริการด้านข้อมูลสำหรับจัดทำรายงานให้กับผู้บริหาร และสนับสนุนการดำเนินงานตอบสนองการแข่งขันของบริษัทรวมถึงสนับสนุนให้รายงานต่าง ๆ มีข้อมูลที่ถูกต้องครบถ้วนและให้ผู้ที่เกี่ยวข้องสามารถใช้งานได้ข้อมูลได้อย่างถูกต้อง

6.1 การจัดหาและบำรุงรักษาแหล่งข้อมูลและรายงานผู้บริหาร

6.1.1 ส่วนงานภายในบริษัทต้องจัดให้มีรายงานผลการดำเนินงานและข้อมูลต่าง ๆ ที่เป็นประโยชน์ต่อการดำเนินธุรกิจแก่ผู้บริหารเพื่อให้ผู้บริหารใช้เป็นข้อมูลในการตัดสินใจต่อการดำเนินงานได้อย่างรวดเร็วและทันเวลา

6.1.2 ส่วนงานภายในบริษัทควรกำหนดให้ข้อมูลในแหล่งข้อมูลและรายงานผู้บริหารมีความสำคัญระดับข้อมูลลับเฉพาะ (Highly Restricted) และห้ามเผยแพรให้ผู้อื่นรับทราบโดยไม่ได้รับอนุญาต

6.1.3 ฝ่ายเทคโนโลยีสารสนเทศ ต้องจัดหาแหล่งข้อมูลเพื่อสนับสนุนให้แต่ละส่วนงานสามารถนำข้อมูลไปใช้ในการวิเคราะห์หรือวิจัยเพื่อใช้ในการแข่งขันทางธุรกิจได้อย่างรวดเร็ว

6.1.4 ฝ่ายเทคโนโลยีสารสนเทศต้องบำรุงรักษาแหล่งข้อมูลและ ผลการดำเนินงานและข้อมูลต่าง ๆ ที่ใช้สำหรับรายงานผู้บริหารให้คงสภาพความถูกต้องและพร้อมใช้อยู่เสมอ

6.1.5 ฝ่ายเทคโนโลยีสารสนเทศต้องสนับสนุนการพัฒนาทักษะของผู้ใช้ข้อมูลแต่ละส่วนงานให้สามารถสร้างรายงานได้อย่างถูกต้องและมีประสิทธิภาพ

6.2 การจัดพิมพ์รายงาน

6.2.1 กรณีที่ผู้ใช้งานต้องการจัดพิมพ์รายงานข้อมูลที่มีความสำคัญสูง ซึ่งหากถูกเผยแพร่ไปยังผู้ที่ไม่เกี่ยวข้องอาจส่งผลกระทบต่อบริษัทอย่างมีนัยสำคัญ ผู้ใช้งานต้องได้รับความเห็นชอบจากผู้บริหารแต่ละฝ่ายงานที่เป็นเจ้าของข้อมูลก่อนดำเนินการทุกครั้ง

6.2.2 ผู้ใช้งานควรมีทะเบียนคุมการพิมพ์รายงาน การจัดส่งรายงาน และการจัดเก็บรายงานต่าง ๆ ที่ได้จัดพิมพ์แล้วอย่างรัดกุม

6.2.3 ผู้ใช้งานควรกำหนดให้มีการลงลายมือชื่อเมื่อมีการรับรายงาน นอกจากนี้ควรทำลายรายงานที่ไม่ได้ใช้งานแล้ว

6.3 การเข้าถึงข้อมูลในแหล่งข้อมูล

6.3.1 ผู้ใช้งานต้องร้องขอสิทธิการใช้งานข้อมูลในแหล่งข้อมูลจากส่วนงานซึ่งเป็นเจ้าของข้อมูลก่อนเข้าถึงแหล่งข้อมูลต่าง ๆ โดยกำหนดกลุ่มของผู้มีสิทธิใช้งานตามขอบเขตข้อมูลเป็น 3 ระดับ ดังนี้

- เข้าถึงข้อมูลทุกหน่วยงาน
- เข้าถึงข้อมูลเฉพาะหน่วยงาน
- เข้าถึงข้อมูลเฉพาะเรื่องที่เกี่ยวข้อง

6.4 การควบคุมคุณภาพของข้อมูลในแหล่งข้อมูล

6.4.1 ผู้ใช้งานต้องรับผิดชอบในการทำข้อมูลให้มีความสมบูรณ์ (Data Cleaning) โดยต้องแจ้งขอข้อมูลเพื่อดำเนินการผ่าน IT Memo และส่งมายังฝ่ายเทคโนโลยีสารสนเทศเพื่อให้เจ้าหน้าที่เทคโนโลยีสารสนเทศดำเนินการดึงข้อมูลและปรับปรุงข้อมูลเข้าระบบ

6.4.2 กรณีที่ผู้ใช้งานต้องการเปลี่ยนแปลงข้อมูลในแหล่งข้อมูล ผู้ใช้งานต้องจัดเตรียมข้อมูลตามกระบวนการทำข้อมูลให้มีความสมบูรณ์ (Data Cleaning) และแจ้งขอดำเนินการเปลี่ยนแปลงข้อมูลผ่าน IT Memo และส่งมายังฝ่ายเทคโนโลยีสารสนเทศเพื่อให้เจ้าหน้าที่เทคโนโลยีสารสนเทศดำเนินการปรับปรุงข้อมูลในฐานข้อมูล

7. การให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บุคคลอื่น (IT Insourcing) และการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)

เพื่อจัดทำข้อกำหนดต่าง ๆ และกรอบการปฏิบัติงานในการให้บริการหรือการใช้บริการด้านงานเทคโนโลยีสารสนเทศของบริษัทให้มีประสิทธิภาพมีความมั่นคงปลอดภัยและเกิดผลประโยชน์สูงสุดแก่บริษัท

7.1 การให้บริการด้านงานเทคโนโลยีสารสนเทศแก่บุคคลอื่น (IT insourcing)

7.1.1 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการควบคุมและกำกับการดำเนินงานด้านเทคโนโลยีสารสนเทศให้เป็นไปตามข้อกำหนดต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจของบริษัท โดยฝ่ายเทคโนโลยีสารสนเทศจะให้บริการทางเทคโนโลยีสารสนเทศภายในบริษัทและบริษัทย่อยเท่านั้น

7.1.2 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการคิดค่าบริการ และค่าธรรมเนียม โดยการคิดค่าบริการและค่าธรรมเนียมต้องได้รับการตกลงร่วมกันระหว่างผู้ให้บริการและผู้ใช้บริการ และสามารถอธิบายที่มาของค่าธรรมเนียมรวมถึงค่าบริการได้ชัดเจนและโปร่งใส

7.1.3 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการควบคุมภายในและจัดทำขั้นตอนการปฏิบัติงาน (Operation Procedure Manual) โดยให้มีการแบ่งแยกอำนาจหน้าที่ของผู้ปฏิบัติงาน (Segregation of Duty) ตามโครงสร้างผู้ปฏิบัติงานที่ชัดเจนและให้บันทึกการปฏิบัติงานนั้นอย่างสม่ำเสมอ

7.1.4 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีมาตรการรองรับเหตุฉุกเฉินโดยจัดให้มีแผนการรองรับเหตุฉุกเฉินและการสำรองข้อมูลรวมถึงกำหนดรอบการสำรองข้อมูลตามที่ตกลงกันไว้กับผู้รับบริการ

7.1.5 ฝ่ายเทคโนโลยีสารสนเทศต้องกำหนดให้มีการสำรองข้อมูลโดยใช้สื่อบันทึกข้อมูลและเก็บสื่อบันทึกข้อมูลในสถานที่ที่ผู้รับบริการจัดหาและเตรียมไว้ให้เป็นการเฉพาะหรือสถานที่ที่ได้ตกลงไว้ร่วมกัน รวมถึงไม่นำข้อมูลการให้บริการของผู้รับบริการไปเผยแพร่หรือนำไปใช้กับบุคคลภายนอก

7.1.6 บริษัทต้องกำหนดให้ผู้ให้บริการมีการบริหารการจัดการระดับการให้บริการตามนโยบายที่กำหนดไว้ใน ข้อ 4. การจัดการระดับการให้บริการ (Service Level Management Policy)

7.2 การใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing)

การจัดหาผู้ให้บริการภายนอกเพื่อให้บริการงานด้านเทคโนโลยีสารสนเทศ ต้องพิจารณาให้มีความสอดคล้องกับกลยุทธ์ทางธุรกิจของบริษัทและคำนึงถึงการให้บริการแก่ลูกค้าอย่างต่อเนื่องและมีความถูกต้องน่าเชื่อถือโดยมีหลักเกณฑ์เบื้องต้นในการใช้บริการจากผู้ให้บริการภายนอก ดังนี้

7.2.1 หลักเกณฑ์ในการพิจารณาการใช้บริการจากผู้ให้บริการภายนอก ต้องไม่ขัดแย้งกับกฎระเบียบหรือข้อกำหนดที่หน่วยงานราชการประกาศใช้

7.2.2 การจัดให้มีการบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management) เพื่อให้มั่นใจว่าระบบสารสนเทศของบริษัทและบริษัทย่อยสามารถดำเนินธุรกิจหรือให้บริการลูกค้าได้อย่างต่อเนื่อง

7.2.3 แนวทางในการพิจารณาคัดเลือกผู้ให้บริการเพื่อประเมินถึงความน่าเชื่อถือของการให้บริการ และเพื่อให้แน่ใจว่าผู้ให้บริการมีความสามารถในการให้บริการได้ตามข้อตกลงการให้บริการ

7.2.4 แนวทางในการรักษาความมั่นคงปลอดภัยและรักษาความลับของข้อมูลเพื่อให้แน่ใจว่าได้ดูแลและรับผิดชอบต่อลูกค้าและมีการคุ้มครองผู้บริโภค (Consumer Protection) อย่างเหมาะสม

7.2.5 การติดตามการประเมินผลและการตรวจสอบการให้บริการจากบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้เป็นไปตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

กำหนดให้มีแนวทางการบริหารความเสี่ยงจากการใช้บริการจากบุคคลภายนอก สำหรับความเสี่ยงด้านปฏิบัติการ (Operational risk) ความเสี่ยงด้านกลยุทธ์ (Strategic risk) ความเสี่ยงด้านชื่อเสียง (Reputational risk) และความเสี่ยงด้านกฎหมาย (Legal risk) โดยกำหนดแนวทางการบริหารความเสี่ยงจากการใช้บริการบุคคลภายนอกเพื่อใช้บริการด้านเทคโนโลยีสารสนเทศไว้อย่างชัดเจนและเป็นลายลักษณ์อักษรให้เหมาะสมกับความสำคัญของระบบงานที่ใช้บริการจากบุคคลภายนอก และสอดคล้องกับนโยบายการบริหารความเสี่ยงโดยรวม รวมทั้งสื่อสารให้บุคคลที่เกี่ยวข้องเข้าใจและถือปฏิบัติตามแนวทางที่กำหนดไว้

นโยบายเทคโนโลยีสารสนเทศฉบับนี้ พิจารณาและอนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 3/2567 เมื่อวันที่ 10 พฤษภาคม 2567 และมีผลบังคับใช้ทันที