

# นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศที่ดี (IT GOVERNANCE POLICY)

## กรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศที่ดี

1. เพื่อให้การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศมีความสอดคล้องกับวัตถุประสงค์และยุทธศาสตร์ขององค์กร (Business Alignment) อย่างมีประสิทธิภาพ มีความโปร่งใส และเป็นไปตามกฎหมาย ข้อบังคับต่างๆขององค์กร จึงให้กำหนดกรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ ของ บสย. ซึ่งประกอบด้วย

- (1) การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงการระบุความเสี่ยง การประเมินความเสี่ยงและการควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้
- (2) การจัดสรรและบริหารทรัพยากรสารสนเทศ ซึ่งครอบคลุมถึงการจัดสรรทรัพยากรให้เพียงพอต่อการดำเนินธุรกิจและการกำหนดแนวทางเพื่อรองรับในกรณีที่ไม่สามารถจัดสรรทรัพยากรให้ได้เพียงพอตามที่กำหนดไว้
- (3) นโยบายความมั่นคงปลอดภัยสารสนเทศและแนวปฏิบัติที่เกี่ยวข้อง
- (4) ความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย

2. เพื่อให้การบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศมีการดำเนินการอย่างมีประสิทธิภาพและเป็นไปในแนวทางเดียวกัน มีความสอดคล้องกับกระบวนการบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management) ให้จัดทำนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และ สื่อสาร บังคับใช้ และปฏิบัติตามนโยบายโดยเคร่งครัด

3. เพื่อให้การส่งมอบผลประโยชน์ (Benefit Delivery) และการใช้ทรัพยากรสารสนเทศได้ประโยชน์สูงสุด (Resource Optimization) เกิดการใช้ทรัพยากรสารสนเทศอย่างคุ้มค่า และตอบสนองต่อความต้องการทางด้านการดำเนินธุรกรรมอย่างมีประสิทธิภาพและประสิทธิผลโดยมีต้นทุนในระดับที่ยอมรับได้ ให้ดำเนินการดังนี้

- (1) ให้จัดทำแผนกลยุทธ์ด้านเทคโนโลยีสารสนเทศขององค์กร โดยให้พิจารณาถึงความสอดคล้องกับแผนกลยุทธ์โดยรวมขององค์กร และให้ครอบคลุมประเด็นความต้องการของผู้มีส่วนได้ส่วนเสีย งบประมาณ ประโยชน์หรือโอกาสและผลตอบแทนที่ได้รับ รวมทั้งความท้าทายที่อาจเกิดขึ้นจากการนำเทคโนโลยีสารสนเทศที่มีอยู่ในปัจจุบันและเทคโนโลยีที่มีการพัฒนาขึ้นมาใหม่มาใช้สำหรับการดำเนินงาน
- (2) ให้จัดทำแนวทางการจัดสรรทรัพยากรสารสนเทศเพื่อเป็นการวางแผนในการจัดสรรทรัพยากรอย่างคุ้มค่า และลดความเสี่ยงที่อาจเกิดขึ้นจากการขาดทรัพยากรสารสนเทศ โดยต้องสอดคล้องกับการจัดสรรทรัพยากรขององค์กรรวมทั้งการบริหารทรัพยากรบุคคลโดยรวมขององค์กรด้วย

4. ให้จัดทำนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและแนวปฏิบัติที่เกี่ยวข้อง พร้อมทั้งดำเนินการสื่อสารให้เกิดการปฏิบัติตามนโยบายโดยเคร่งครัด

5. เพื่อให้เกิดความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder Transparency) ต้องจัดให้มีการรายงานและการสื่อสารผลการดำเนินงานและการบริหารจัดการเทคโนโลยีสารสนเทศกับผู้มีส่วนได้ส่วนเสียอย่างมีประสิทธิภาพ โดยให้พิจารณาถึงการประเมินความต้องการของผู้มีส่วนได้ส่วนเสีย รวมทั้ง รูปแบบ กลยุทธ์ และ ช่องทางการสื่อสารที่เหมาะสม