



การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

แนวปฏิบัติประกอบนโยบาย
การกำกับดูแลด้านเทคโนโลยีสารสนเทศ
(IT Governance Procedure)

รหัสเอกสาร : ITG-SD-001

เวอร์ชัน : 3.0

สำนักดิจิทัล

ฝ่ายกลยุทธ์ดิจิทัลและบริหารจัดการข้อมูล

กองกลยุทธ์ดิจิทัล

อนุมัติ

(ลงชื่อ).....

(.....นายเกรียงศักดิ์ กิตติประภัสร์.....)

ตำแหน่ง.....รองผู้อำนวยการสารสนเทศและสื่อสาร.....

5 / ม.ค. / 2566

A-WM-01

ประวัติการปรับปรุงเอกสาร

เวอร์ชัน	วันที่มีผลบังคับใช้	ผู้ดำเนินการ	รายละเอียด
1.0	29 ธ.ค. 2563	กตท.	ออกเอกสารครั้งแรก
1.1	1 เม.ย. 2564	กตท.	ทบทวนครั้งที่ 1 ปรับปรุงเพิ่มเติมตามผลการตรวจสอบภายใน ITG (ITG Internal Audit) ปี 2564 - ความถี่ในการทบทวนเอกสาร - ขยายความเพิ่มเติมในหมวด 2-4 เพื่อให้มั่นใจได้ว่ากระบวนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศครอบคลุมถึงด้าน ความมั่นคงปลอดภัยสารสนเทศ การจัดการการเปลี่ยนแปลง การจัดการเหตุขัดข้อง และการบริหารความเสี่ยงทางธุรกิจ
2.0	28 ก.พ. 2565	กตท.	ทบทวนครั้งที่ 2 ขยายความเพิ่มเติมในหมวด 2 เพื่อให้มั่นใจได้ว่าการกำกับดูแลครอบคลุมถึงเรื่อง การจัดการคุณภาพด้านเทคโนโลยีสารสนเทศ
3.0	5 ม.ค. 2566	กตท.	ทบทวนครั้งที่ 3 ปรับปรุงแนวทางการดำเนินงาน ให้ผู้ที่เกี่ยวข้องสามารถดำเนินการตามหลักการ ITG

สารบัญ

	หน้า
1. บทนำ.....	1
2. วัตถุประสงค์	1
3. ขอบเขต	2
4. นิยามและคำจำกัดความ	2
5. การดำเนินการตามนโยบายการกำกับดูแลด้านเทคโนโลยีสารสนเทศ.....	5
6. แนวทางดำเนินงานด้านการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ	5
6.1 หลักการกำกับดูแลด้านเทคโนโลยีสารสนเทศ	5
6.2 แนวปฏิบัติที่ดีในการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ	17
7. ภาคผนวก	18
7.1 มาตรฐานและแนวปฏิบัติอ้างอิง	18

1. บทนำ

การไฟฟ้าส่วนภูมิภาค (กฟภ.) ตระหนักถึงความสำคัญในการใช้เทคโนโลยีสารสนเทศให้มีประสิทธิภาพ ประสิทธิภาพ และเป็นที่ยอมรับ ตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสียในการดำเนินธุรกิจและภารกิจของการไฟฟ้าส่วนภูมิภาค มีการกำกับดูแล การบริหารจัดการด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง ตามหลักการกำกับดูแลกิจการที่ดี รวมทั้งมีการบริหารจัดการที่ดีเลิศและบูรณาการตามแนวทางการกำกับดูแล การบริหารความเสี่ยง และการปฏิบัติตามกฎเกณฑ์ (Integrated GRC: Governance Risk and Compliance)

ปัจจุบัน การไฟฟ้าส่วนภูมิภาคได้นำหลักการและแนวทางการปฏิบัติตามมาตรฐานสากลและแนวปฏิบัติที่ดีเลิศ (Standards and Best Practices) ได้แก่ มาตรฐาน ISO/IEC 38500 (Governance of IT for the Organization) และ COBIT 2019 (A Business Framework for the Governance and Management of Enterprise IT) มาใช้ในการกำกับดูแลและการบริหารจัดการด้านเทคโนโลยีสารสนเทศ ที่มีการกำหนด ทิศทางและควบคุม โดยมีการประเมิน (Evaluate) สั่งการ (Direct) และติดตามผล (Monitor) สำหรับ การจัดการเทคโนโลยีสารสนเทศทั้งในปัจจุบันและอนาคต ตั้งแต่การวางแผน ออกแบบ พัฒนา ติดตั้งใช้งาน ปฏิบัติงาน บริหารจัดการ และประยุกต์ใช้เทคโนโลยีสารสนเทศ โดยการกำกับดูแลด้านเทคโนโลยีสารสนเทศ ของการไฟฟ้าส่วนภูมิภาค ได้ยึดหลักการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (Principles for Good Governance of IT) ตามมาตรฐานสากล ISO/IEC 38500 ดังนี้

- (1) หลักการด้านความรับผิดชอบ (Responsibility)
- (2) หลักการด้านยุทธศาสตร์ (Strategy)
- (3) หลักการด้านการจัดหา (Acquisition)
- (4) หลักการด้านผลการดำเนินงาน (Performance)
- (5) หลักการด้านผลความสอดคล้องตามข้อกำหนด (Conformance)
- (6) หลักการด้านพฤติกรรมบุคคล (Human Behavior)

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Governance, ITG) อย่างเป็นระบบ จะเป็นกลไก สำคัญในการสนับสนุนการกำกับดูแลกิจการที่ดี (Corporate Governance) ทั้งในเรื่องของการกำหนด นโยบาย มาตรฐาน และแนวปฏิบัติ เพื่อสร้างความเชื่อมั่นในการให้บริการด้านเทคโนโลยีสารสนเทศ การจัดการ ความเสี่ยง และการสร้างโอกาสทางธุรกิจจากการนำระบบเทคโนโลยีสารสนเทศมาใช้ รวมไปถึงเรื่องของการ ปฏิบัติงานที่สอดคล้องกับกฎหมาย ข้อบังคับ กฎ ระเบียบ และข้อกำหนดต่าง ๆ อันจะเป็นการสร้าง คุณค่าจากการใช้งานเทคโนโลยีสารสนเทศ ตลอดจนสนับสนุนการดำเนินงานตามแผนงานและยุทธศาสตร์ การไฟฟ้าส่วนภูมิภาคให้เป็นไปอย่างมีประสิทธิภาพ

2. วัตถุประสงค์

เพื่อให้การไฟฟ้าส่วนภูมิภาคมีการกำกับดูแลและการบริหารจัดการด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องตามมาตรฐานสากลและแนวปฏิบัติที่ดีเลิศ มีแนวทางการปฏิบัติให้ผู้บริหาร พนักงาน ลูกจ้าง และผู้ปฏิบัติงานให้การไฟฟ้าส่วนภูมิภาค ได้รับทราบและยึดถือปฏิบัติในการดำเนินการที่เกี่ยวข้องกับ การใช้เทคโนโลยีสารสนเทศ อันจะเป็นการดำรงไว้ซึ่งการกำกับดูแลและบริหารจัดการด้านเทคโนโลยี สารสนเทศของการไฟฟ้าส่วนภูมิภาค

3. ขอบเขต

นโยบายฉบับนี้ครอบคลุมแนวทางการปฏิบัติสำหรับผู้บริหาร พนักงาน ลูกจ้าง และผู้ปฏิบัติงานให้การไฟฟ้าส่วนภูมิภาค ในการดำเนินการที่เกี่ยวข้องกับการจัดการเทคโนโลยีสารสนเทศ ทั้งด้านการให้บริการและการใช้งาน เพื่อให้มั่นใจได้ว่าการจัดการเทคโนโลยีสารสนเทศสามารถส่งเสริมให้เกิดผลสำเร็จในการปฏิบัติงานของการไฟฟ้าส่วนภูมิภาคได้อย่างแท้จริง โดยพิจารณาจากสิ่งต่าง ๆ ดังนี้

- นวัตกรรมในการบริการและธุรกิจ
- ความสอดคล้องของเทคโนโลยีสารสนเทศกับความต้องการทางธุรกิจ
- การนำไปใช้และการดำเนินการที่เกี่ยวข้องกับทรัพย์สินสารสนเทศอย่างเหมาะสม
- ความชัดเจนในหน้าที่รับผิดชอบและภาระรับผิดชอบ ทั้งสำหรับอุปสงค์และอุปทานของเทคโนโลยีสารสนเทศในการบรรลุเป้าประสงค์ขององค์กร
- ความต่อเนื่องทางธุรกิจและความยั่งยืน
- การจัดสรรทรัพยากรอย่างมีประสิทธิภาพ
- แนวปฏิบัติที่ดีในด้านความสัมพันธ์กับผู้มีส่วนได้ส่วนเสีย
- การรับรู้ประโยชน์ที่ได้รับจากการลงทุนด้านเทคโนโลยีสารสนเทศในแต่ละครั้ง

4. นิยามและคำจำกัดความ

1. “ผู้มีส่วนได้ส่วนเสีย” (Stakeholder) หมายความว่า บุคคล กลุ่มบุคคล หรือหน่วยงานองค์กรใด ๆ ทั้งภายในและภายนอกองค์กร ที่อาจมีผลหรือได้รับผล หรือรับรู้ว่าจะได้รับผลกระทบจากการตัดสินใจหรือกิจกรรมของการไฟฟ้าส่วนภูมิภาค ได้แก่ หน่วยงานกำกับดูแล พนักงาน ผู้ส่งมอบ คู่ค้า คู่ความร่วมมือ ลูกค้า/ผู้ใช้บริการ และชุมชน สังคม และสิ่งแวดล้อม

2. “ผู้รับผิดชอบการกำกับดูแล” (Governing Bodies) หมายความว่า บุคคลหรือกลุ่มบุคคล ซึ่งมีภาระรับผิดชอบต่อผลดำเนินการขององค์กร ทั้งผลด้านการปฏิบัติงาน (Performance) และผลด้านความสอดคล้องต่อข้อกำหนด (Conformance) ได้แก่ คณะกรรมการ/คณะทำงานที่ได้รับการแต่งตั้งเพื่อดำเนินการในเรื่องการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

3. “ผู้บริหารด้านเทคโนโลยีสารสนเทศ” หมายความว่า บุคคลหรือกลุ่มบุคคลที่มีหน้าที่บริหารจัดการภายใต้อำนาจหน้าที่และภาระรับผิดชอบที่กำหนดขึ้นจากการกำกับดูแล (Governance) เพื่อให้บรรลุวัตถุประสงค์ขององค์กร

4. “ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ” หมายความว่า บุคคลหรือกลุ่มบุคคลที่มีหน้าที่ดำเนินการและตัดสินใจเพื่อให้บรรลุผลลัพธ์ด้านเทคโนโลยีสารสนเทศที่ต้องการ มีความรับผิดชอบต่อการปฏิบัติงานตามหน้าที่หรือตามที่มอบหมาย ให้บรรลุผลตามที่กำหนด

5. “การกำกับดูแล” (Governance) หมายความว่า การกำหนดนโยบาย การติดตามผลการดำเนินการอย่างต่อเนื่องโดยผู้รับผิดชอบการกำกับดูแล

6. “การกำกับดูแลด้านเทคโนโลยีสารสนเทศ” (Governance of IT, IT Governance, ITG, Govern IT) หมายความว่า หลักการบริหารจัดการเทคโนโลยีสารสนเทศ และสนับสนุนการดำเนินงานทางด้านสารสนเทศอย่างมีประสิทธิภาพและประสิทธิผล ทั้งยังกำหนดให้มีทิศทางและการควบคุม โดยจัดให้มี

การประเมิน (Evaluate) สั่งการ (Direct) และติดตามผล (Monitor) สำหรับการใช้เทคโนโลยีสารสนเทศขององค์กรทั้งในปัจจุบันและอนาคต

7. “การบริหารจัดการทรัพยากรเทคโนโลยีสารสนเทศ” (IT Resource Management) หมายความว่า การวางแผน การออกแบบ การพัฒนา การติดตั้งใช้งาน การปฏิบัติงาน การบริหารจัดการ และการประยุกต์ใช้เทคโนโลยีสารสนเทศ เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจ และสร้างคุณค่าให้กับองค์กร โดยมีความหมายทั้งในด้านความต้องการใช้และการให้บริการ

8. “เทคโนโลยีสารสนเทศ” (Information Technology: IT) หมายความว่า ทรัพยากรที่ใช้ในการได้มา ประมวล จัดเก็บ และเผยแพร่สารสนเทศ โดย “IT” มีความหมายครอบคลุมถึง “เทคโนโลยีการสื่อสาร” (Communications Technology: CT) และ “เทคโนโลยีสารสนเทศและการสื่อสาร” (Information and Communications Technology: ICT)

9. “การบริหารจัดการ” (Management) หมายความว่า การดำเนินการในการควบคุม (Control) และ ควบคุมดูแล (Supervision) ภายใต้อำนาจหน้าที่และภาระรับผิดชอบที่กำหนดขึ้นจากการกำกับดูแล (Governance) เพื่อให้บรรลุวัตถุประสงค์ขององค์กร การบริหารจัดการให้มีประสิทธิภาพและประสิทธิผลประกอบด้วย

- 1) วางแผน (Plan): การออกแบบ วางแผน จัดโครงสร้างที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ ดำเนินการสอดคล้องตามกฎหมาย
- 2) จัดทำ (Build): การจัดสร้าง จัดทำให้ได้มาซึ่งระบบหรือเทคโนโลยีสารสนเทศ บริหารการเปลี่ยนแปลง และนำไปติดตั้งสำหรับการใช้งาน
- 3) ดำเนินการ (Run): การส่งมอบบริการ ให้บริการ ดำเนินการ ปฏิบัติงาน และสนับสนุนในการให้บริการที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ
- 4) เฝ้าติดตาม (Monitor): การติดตามผลดำเนินการหรือผลการปฏิบัติงาน ประเมินผลตามข้อตกลงหรือเกณฑ์ที่กำหนด และประเมินตามรายการอ้างอิงของข้อกำหนดต่าง ๆ

10. “ภาระรับผิดชอบ” (Accountability) หมายความว่า สถานะของการมีภาระรับผิดชอบต่อผลสัมฤทธิ์หรือความสำเร็จของงาน

11. “หน้าที่รับผิดชอบ” (Responsibility) หมายความว่า พันธะผูกพันที่จะต้องดำเนินการและตัดสินใจเพื่อให้บรรลุผลลัพธ์ที่ต้องการ ความรับผิดชอบต่อการทำงานตามหน้าที่หรือตามที่ได้รับมอบหมาย ให้บรรลุผลตามที่กำหนด

12. “แผนงาน” หรือ “แผนโครงการ” (Programme) หมายความว่า แผนการปฏิบัติงาน แผนธุรกิจ หรือข้อมูลที่แสดงถึงประโยชน์ที่จะได้รับ งบประมาณ ความเสี่ยงและ โอกาสทางธุรกิจ รวมถึงปัจจัยต่าง ๆ เพื่อให้ฝ่ายบริหารสามารถใช้ในการตัดสินใจ

13. “โครงการ” (Project) หมายความว่า การดำเนินกิจกรรมซึ่งมีการกำหนดวัตถุประสงค์ ระยะเวลา งบประมาณ กระบวนการและกิจกรรมเป็นลำดับอย่างชัดเจน และมีผู้รับผิดชอบ บริหารงาน เพื่อให้กิจกรรมต่าง ๆ เป็นไปตามแผนงาน เหมาะสมกับเวลาและงบประมาณที่ตั้งไว้

14. “ทรัพยากร” (Resources) หมายความว่า บุคลากร กระบวนการ วิธีปฏิบัติ ระบบงานหรือซอฟต์แวร์ ข้อมูลสารสนเทศ อุปกรณ์ วัสดุสิ้นเปลือง ระบบโครงสร้างพื้นฐาน เงินทุน งบประมาณค่าใช้จ่ายในการดำเนินการ และเวลา

15. “ปัจจัยภายใน” หมายความว่า ปัจจัยขับเคลื่อนหรือบริบทภายในองค์กร สภาพแวดล้อมภายในองค์กร ที่มีผลต่อการบรรลุวัตถุประสงค์ขององค์กร ได้แก่

- 1) การกำกับดูแล โครงสร้างองค์กร บทบาท และภาระรับผิดชอบ
- 2) เป้าหมาย เป้าประสงค์ทางธุรกิจ
- 3) ยุทธศาสตร์ทางธุรกิจ
- 4) การบริหารความเสี่ยง เกณฑ์ความเสี่ยงที่ยอมรับได้
- 5) วัฒนธรรมขององค์กร
- 6) ระดับความสามารถขององค์กร ทักษะ การจัดฝึกอบรม และขีดความสามารถ ของการใช้เทคโนโลยีสารสนเทศ
- 7) แผนงานการเปลี่ยนแปลงทางกลยุทธ์
- 8) ความต้องการในเชิงนวัตกรรมด้านการจัดการเทคโนโลยีสารสนเทศ เพื่อความได้เปรียบในการแข่งขันทางธุรกิจ
- 9) การรายงานผลเพื่อสร้างความเชื่อมั่น โดยครอบคลุมถึงการตรวจสอบและความเสี่ยง
- 10) วิธีปฏิบัติสำหรับกระบวนการทางธุรกิจที่สำคัญ ซึ่งสนับสนุนโดยเทคโนโลยีสารสนเทศ
- 11) บริการที่สำคัญด้านเทคโนโลยีสารสนเทศ และแนวปฏิบัติการให้บริการ
- 12) แนวทางดำเนินการร่วมกับคู่ค้าและหน่วยงานภายนอก

16. “ปัจจัยภายนอก” หมายความว่า ปัจจัยขับเคลื่อนหรือบริบทภายนอกองค์กร สภาพแวดล้อมภายนอกองค์กรที่มีผลต่อการบรรลุวัตถุประสงค์ขององค์กร ได้แก่

- 1) ข้อกำหนดที่มีผลบังคับใช้ตามกฎหมาย กฎ ระเบียบ ข้อบังคับ ข้อตกลง
- 2) การเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศ
- 3) แนวโน้มทางเศรษฐกิจและสังคม
- 4) ขีดความสามารถและความพร้อมด้านทักษะ ความสามารถ
- 5) ปัจจัยในการแข่งขันทางธุรกิจ
- 6) สภาพแวดล้อมทางธุรกิจและการตลาด
- 7) ข้อกำหนดความต้องการของผู้มีส่วนได้ส่วนเสีย
- 8) ภัยคุกคามและประเด็นความเสี่ยงด้านเทคโนโลยีสารสนเทศ
- 9) การเปลี่ยนแปลงสภาพทางภูมิอากาศ

17. “ทรัพย์สินสารสนเทศ” หมายความว่า สินทรัพย์/ทรัพย์สิน ที่เป็นระบบและอุปกรณ์ประเภทซอฟต์แวร์ ฮาร์ดแวร์ ข้อมูลและสารสนเทศ ทั้งที่อยู่ในรูปอิเล็กทรอนิกส์ เอกสาร และข้อความเสี่ยง โดยประกอบด้วย

- 1) ทรัพย์สินสารสนเทศประเภทระบบ ได้แก่ ระบบเครือข่ายสื่อสาร ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ และระบบงานธุรกิจ
- 2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์ต่อพ่วงอื่นใด
- 3) ทรัพย์สินสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

5. การดำเนินการตามนโยบายการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

การไฟฟ้าส่วนภูมิภาคได้กำหนดนโยบายการกำกับดูแลด้านเทคโนโลยีสารสนเทศ และมีแนวทางการดำเนินการตามนโยบายฯ ดังต่อไปนี้

1. กำหนดให้มีโครงสร้างการกำกับดูแลด้านเทคโนโลยีสารสนเทศ พร้อมทั้งกำหนดบทบาทและหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง
2. กำหนดให้มีการจัดทำแนวทางหรือขั้นตอนปฏิบัติเพื่อกำกับดูแลด้านเทคโนโลยีสารสนเทศ ให้เป็นไปตามมาตรฐานสากล ISO/IEC 38500 และกรอบการดำเนินงาน COBIT 2019
3. กำหนดแนวทางและส่งเสริมให้หน่วยงานที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ ปฏิบัติตามแนวทางหรือขั้นตอนการกำกับดูแลด้านเทคโนโลยีสารสนเทศของการไฟฟ้าส่วนภูมิภาค
4. กำหนดให้มีการติดตามผลการกำกับดูแลด้านเทคโนโลยีสารสนเทศอยู่เสมอ และรายงานให้คณะกรรมการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (IT Governance Committee) อยู่เสมอ เพื่อพิจารณาให้ข้อคิดเห็น
5. กำหนดให้มีการตรวจสอบ การตรวจติดตามการนำไปปฏิบัติตามนโยบาย แนวปฏิบัติ และกระบวนการ โดยให้ความเป็นอิสระในการตรวจสอบ รายงานให้คณะกรรมการ กฟผ. อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อพิจารณาให้ข้อคิดเห็น
6. กำหนดให้มีการทบทวนนโยบายการกำกับดูแลด้านเทคโนโลยีสารสนเทศ แนวปฏิบัติประกอบนโยบายฯ บริบทการกำกับดูแลด้านเทคโนโลยีสารสนเทศ คู่มือการกำกับดูแลด้านเทคโนโลยีสารสนเทศ ข้อกำหนดสำหรับผลลัพธ์ เกณฑ์วัด และวิธีการประเมินการกำกับดูแลด้านเทคโนโลยีสารสนเทศ (ITG Beneficial Outcomes) และเอกสารที่เกี่ยวข้อง อย่างน้อยปีละ 1 ครั้ง

6. แนวทางดำเนินงานด้านการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ

6.1 หลักการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

การกำกับดูแลด้านเทคโนโลยีสารสนเทศของการไฟฟ้าส่วนภูมิภาค ดำเนินการตามหลักการ 6 ด้านตามมาตรฐานสากล ISO/IEC 38500:2015 ดังนี้

- ด้านที่ 1 หลักการด้านความรับผิดชอบ (Responsibility)
- ด้านที่ 2 หลักการด้านยุทธศาสตร์ (Strategy)
- ด้านที่ 3 หลักการด้านการจัดหา (Acquisition)
- ด้านที่ 4 หลักการด้านผลการดำเนินงาน (Performance)
- ด้านที่ 5 หลักการด้านผลความสอดคล้องตามข้อกำหนด (Conformance)
- ด้านที่ 6 หลักการด้านพฤติกรรมบุคคล (Human Behavior)

ด้านที่ 1 หลักการด้านความรับผิดชอบ (Responsibility)

หลักการ

พิจารณาแต่งตั้งให้มีบุคคลที่มีหน้าที่รับผิดชอบเพื่อจัดการความต้องการในการใช้เทคโนโลยีสารสนเทศ และจัดให้มีบริการที่จำเป็นตามความต้องการนั้นทั้งในปัจจุบันและอนาคต โดยต้องมีการกำหนดอำนาจหน้าที่ในการดำเนินงานอย่างเหมาะสม เป็นไปตามแนวทางเดียวกันกับยุทธศาสตร์องค์กร

แนวปฏิบัติสำหรับผู้รับผิดชอบการกำกับดูแล

ประเมิน (Evaluate)

(1) ผู้รับผิดชอบการกำกับดูแล กำหนดให้มีกฎบัตร หรือคำบรรยายลักษณะงาน (Job Description) ของผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศ ให้มั่นใจได้ว่าการจัดการเทคโนโลยีสารสนเทศ ภายในองค์กรเกิดประสิทธิภาพ ประสิทธิผล รวมทั้งสนับสนุนวัตถุประสงค์การดำเนินงานของการไฟฟ้าส่วนภูมิภาค ทั้งในปัจจุบันและอนาคต

(2) ผู้รับผิดชอบการกำกับดูแล ประเมินความสามารถของผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

สั่งการ (Direct)

(1) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้ผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศ ปฏิบัติหน้าที่ตามยุทธศาสตร์ของการไฟฟ้าส่วนภูมิภาค

(2) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้ผู้มีหน้าที่รับผิดชอบด้านเทคโนโลยีสารสนเทศ ต้องได้รับข้อมูลที่จำเป็นในการปฏิบัติงานเพื่อให้บรรลุเป้าหมายที่วางไว้ โดยผู้รับผิดชอบการกำกับดูแลให้สิทธิแก่ผู้มีหน้าที่รับผิดชอบด้านเทคโนโลยีสารสนเทศในการเข้าถึงข้อมูลที่จำเป็น หรือมอบหมายหน้าที่ในการสนับสนุนข้อมูลที่จำเป็นแก่ผู้มีหน้าที่รับผิดชอบด้านเทคโนโลยีสารสนเทศท่านอื่น

ติดตามผล (Monitor)

(1) ผู้รับผิดชอบการกำกับดูแล ติดตาม ประเมินความเหมาะสมของการกำหนดโครงสร้าง และการแบ่งแยกหน้าที่ว่ามีความเหมาะสมหรือไม่ รวมทั้งผลการดำเนินงานของผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศ นอกจากนี้ควรประเมินความเข้าใจในบทบาทหน้าที่และความรับผิดชอบของผู้ที่ได้รับมอบหมายด้วย

(2) ผู้รับผิดชอบการกำกับดูแล ติดตามผลการดำเนินงานของผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศ รวมถึงความสามารถในการปฏิบัติงานและเสนอแผนงานที่เป็นประโยชน์เพื่อส่งเสริมการกำกับดูแลด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการผู้รับผิดชอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

แนวปฏิบัติสำหรับผู้บริหารและผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

สำหรับผู้บริหารด้านเทคโนโลยีสารสนเทศ จะประเมินและกำหนดบทบาทหน้าที่ ความรับผิดชอบ และโครงสร้างการดำเนินงาน จากนั้นมอบหมายให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ดำเนินงานตามบทบาทหน้าที่อย่างมีประสิทธิภาพ ประสิทธิผล เพื่อให้สามารถบรรลุผลสำเร็จตามยุทธศาสตร์และนโยบายของ กฟภ. รวมถึงตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสียอย่างครบถ้วนต่อไป โดยผู้บริหารด้านเทคโนโลยีสารสนเทศ จะติดตามและประเมินผลการดำเนินงาน เพื่อให้มั่นใจว่าผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ มีความเข้าใจในบทบาทหน้าที่และสามารถดำเนินงานได้อย่างมีประสิทธิภาพ ประสิทธิผล

ด้านที่ 2 หลักการด้านยุทธศาสตร์ (Strategy)

หลักการ

พิจารณาถึงขีดความสามารถและแผนงานด้านเทคโนโลยีสารสนเทศ ทั้งในปัจจุบันและอนาคต เพื่อตอบสนองความต้องการตามยุทธศาสตร์ขององค์กร

แนวปฏิบัติสำหรับผู้รับผิดชอบการกำกับดูแล

ประเมิน (Evaluate)

(1) ผู้รับผิดชอบการกำกับดูแล ประเมินการพัฒนาด้านเทคโนโลยีสารสนเทศ และกระบวนการทำงานขององค์กร เพื่อให้มั่นใจได้ว่าจะมีความสอดคล้องและสนับสนุนแผนงานของการไฟฟ้าส่วนภูมิภาค ทั้งในปัจจุบันและในอนาคต

(2) ผู้รับผิดชอบการกำกับดูแล ประเมินการจัดการเทคโนโลยีสารสนเทศและกิจกรรมด้านเทคโนโลยีสารสนเทศ ตลอดจนการจัดการคุณภาพด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นส่วนหนึ่งในการจัดทำแผนงานและนโยบาย เพื่อให้มั่นใจได้ว่าการดำเนินการเกี่ยวกับเทคโนโลยีสารสนเทศนั้นสอดคล้องเป็นไปในแนวทางเดียวกับวัตถุประสงค์ขององค์กรและอยู่ในระดับความเสี่ยงที่เหมาะสม รวมทั้งตอบสนองต่อความต้องการหลักของผู้มีส่วนได้ส่วนเสียที่แท้จริง ทั้งนี้ให้นำแนวปฏิบัติที่ดีมาใช้ในการปฏิบัติงานจริงด้วย

สั่งการ (Direct)

(1) ผู้รับผิดชอบการกำกับดูแล มอบหมาย สั่งการให้มีการพัฒนาด้านเทคโนโลยีสารสนเทศ โดยต้องสอดคล้องกับยุทธศาสตร์และแผนปฏิบัติการดิจิทัล ตลอดจนการนำแผนปฏิบัติการดิจิทัลไปใช้ในการปฏิบัติงานจริง โดยคำนึงถึงการวางแผนเพื่อให้มีการจัดการคุณภาพด้านเทคโนโลยีสารสนเทศที่ครอบคลุมกระบวนการที่สำคัญขององค์กร อาทิเช่น การกำกับดูแลด้านเทคโนโลยีสารสนเทศ การจัดการความมั่นคงปลอดภัยสารสนเทศ การจัดการบริการด้านเทคโนโลยีสารสนเทศ การบริหารความเสี่ยงทางธุรกิจ การกำกับดูแลข้อมูล การขับเคลื่อนแผนงาน/โครงการด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจได้ว่าองค์กรได้รับประโยชน์สูงสุดจากการพัฒนาด้านเทคโนโลยีสารสนเทศ

(2) ผู้รับผิดชอบการกำกับดูแล ส่งเสริมให้ผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศนำเสนอข้อเสนอแผนงานการพัฒนาด้านเทคโนโลยีสารสนเทศ เพื่อให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยี ซึ่งจะช่วยให้องค์กรสามารถตอบสนองต่อความท้าทาย และเพิ่มโอกาสในการแข่งขันทางธุรกิจ

ติดตามผล (Monitor)

(1) ผู้รับผิดชอบการกำกับดูแล ติดตามผลของการจัดการเทคโนโลยีสารสนเทศ ตลอดจนการจัดการคุณภาพด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าองค์กรได้รับประโยชน์ตามเป้าหมายที่กำหนดไว้ในข้อเสนอแผนงาน

(2) ผู้รับผิดชอบการกำกับดูแล ติดตามสถานะความคืบหน้าของข้อเสนอแผนงานด้านเทคโนโลยีสารสนเทศตามที่ได้รับอนุมัติอย่างต่อเนื่อง เพื่อให้มั่นใจได้ว่าข้อเสนอแผนงานนั้นได้ดำเนินการตามวัตถุประสงค์ภายใต้กรอบเวลาและทรัพยากรตามที่ได้รับจัดสรรไว้อย่างเหมาะสม

แนวปฏิบัติสำหรับผู้บริหารและปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

สำหรับผู้บริหารด้านเทคโนโลยีสารสนเทศ จะประเมินและกำหนดยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศที่สอดคล้องและสนับสนุนยุทธศาสตร์ของ กฟผ. ซึ่งครอบคลุมแผนงาน/โครงการต่าง ๆ จากนั้น

มอบหมายให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ นำแผนงาน/โครงการตามยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ ไปปฏิบัติโดยดำเนินการต่อไป ดังนี้

- ระบุผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง และรวบรวมข้อกำหนดความต้องการจากผู้มีส่วนได้ส่วนเสีย
- ศึกษาความเป็นไปได้ในการดำเนินงาน วิเคราะห์ผลตอบแทนที่คาดว่าจะได้รับ และประเมินความเสี่ยงที่คาดว่าจะเกิดขึ้น
- กำหนดขอบเขตงาน เทคโนโลยีที่เลือกใช้ ชัดความสามารถที่จำเป็นของบุคลากร ผลประโยชน์ที่คาดว่าจะได้รับ ตัวชี้วัดผลสำเร็จสอดคล้องกับเป้าหมายที่กำหนด และกรอบงบประมาณ ให้ชัดเจน
- ขออนุมัติดำเนินการต่อผู้บริหารด้านเทคโนโลยีสารสนเทศ

โดยผู้บริหารด้านเทคโนโลยีสารสนเทศ จะติดตามและประเมินผลการดำเนินงาน เพื่อให้มั่นใจว่าผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ มีแนวทางที่เหมาะสมในการดำเนินงานตามแผนงาน/โครงการตามยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถบรรลุผลสำเร็จตามวัตถุประสงค์

ด้านที่ 3 หลักการด้านการจัดหา (Acquisition)

หลักการ

พิจารณาให้มีการจัดหาเทคโนโลยีสารสนเทศอย่างสมเหตุสมผล บนพื้นฐานของการวิเคราะห์อย่างเหมาะสมและต่อเนื่อง ด้วยการตัดสินใจที่ชัดเจนและโปร่งใส มีความสมดุลที่เหมาะสมระหว่างประโยชน์ที่ได้รับ โอกาสทางธุรกิจ ค่าใช้จ่าย และความเสี่ยง ทั้งในระยะสั้นและระยะยาว

แนวปฏิบัติสำหรับผู้รับผิดชอบการกำกับดูแล

ประเมิน (Evaluate)

(1) ผู้รับผิดชอบการกำกับดูแล ประเมินทางเลือกสำหรับการจัดซื้อ จัดหา จัดจ้างเทคโนโลยีสารสนเทศ ตามข้อเสนอแผนงานที่ได้รับอนุมัติ โดยพิจารณาถึงความเหมาะสมถึงความเสี่ยงและความคุ้มค่าจากการลงทุน

สั่งการ (Direct)

(1) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้ผู้รับผิดชอบจัดหาทรัพยากรสารสนเทศที่จำเป็นอย่างเหมาะสม รวมถึงกำหนดแนวทางหรือวิธีปฏิบัติในการจัดหาเป็นลายลักษณ์อักษร

(2) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้ผู้รับผิดชอบในเรื่องการจัดหา (ทั้งการจัดหาจากภายในและจากภายนอก) เพื่อให้ดำเนินการสอดคล้องกับความต้องการทางธุรกิจขององค์กร โดยคำนึงถึงการออกแบบหรือพัฒนาเพื่อให้มีการจัดการความมั่นคงปลอดภัยสารสนเทศ การจัดการการเปลี่ยนแปลง การจัดการเหตุขัดข้อง และการบริหารความเสี่ยงทางธุรกิจอย่างมีประสิทธิภาพด้วย รวมทั้งสั่งการให้ผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศ สื่อสารและทำความเข้าใจถึงวัตถุประสงค์ขององค์กรในการจัดหาเทคโนโลยีสารสนเทศร่วมกับบุคคลที่เกี่ยวข้องทั้งในองค์กรและผู้ให้บริการภายนอก

ติดตามผล (Monitor)

(1) ผู้รับผิดชอบการกำกับดูแล ติดตามผลดำเนินงานที่ได้มีการลงทุนด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจได้ว่าผลลัพธ์เป็นไปตามดัชนีชี้วัดและเกิดประโยชน์ตามที่ผู้มีส่วนได้ส่วนเสียคาดหวัง

(2) ผู้รับผิดชอบการกำกับดูแล ติดตามขอบเขตของการสื่อสารและทำความเข้าใจที่เกิดขึ้นระหว่างบุคคลที่เกี่ยวข้องในองค์กรและผู้ให้บริการภายนอก

แนวปฏิบัติสำหรับผู้บริหารและปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

สำหรับผู้บริหารด้านเทคโนโลยีสารสนเทศ จะประเมินและกำหนดแนวทางการจัดหา/พัฒนาระบบเทคโนโลยีสารสนเทศที่สมเหตุสมผล โปร่งใส และเกิดประโยชน์คุ้มค่า จากนั้นมอบหมายให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศดำเนินการต่อไป ดังนี้

- พิจารณารูปแบบที่เหมาะสมในการจัดหา/พัฒนาระบบเทคโนโลยีสารสนเทศ ว่าจะดำเนินการเองหรือจ้างผู้ให้บริการภายนอก เพื่อให้เกิดประโยชน์คุ้มค่าสูงสุดต่อ กฟผ. โดยในกรณีที่มีการจัดซื้อจัดจ้างจะต้องดำเนินการให้สอดคล้องตามกฎหมาย ระเบียบ คำสั่ง ข้อบังคับต่าง ๆ ที่เกี่ยวข้องกับการจัดซื้อจัดจ้างอย่างครบถ้วน ตลอดจนบริหารสัญญาและตรวจรับให้เป็นไปตามขอบเขตงาน (TOR)
- ออกแบบ พัฒนา ทดสอบและนำระบบเทคโนโลยีสารสนเทศออกใช้งานโดยเลือกใช้เครื่องมือที่เหมาะสมในการพัฒนาระบบฯ และมีการจัดทำคู่มือการใช้งาน ทั้งนี้ ต้องคำนึงถึงความสอดคล้อง

กับข้อกำหนดที่เกี่ยวข้องด้วย เช่น ด้านสถาปัตยกรรมองค์กร ด้านความมั่นคงปลอดภัยสารสนเทศ ด้านข้อมูลส่วนบุคคล

- รายงานความก้าวหน้าของการดำเนินงานต่อผู้บริหารด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ ตามรอบการรายงาน และแก้ไขปัญหาอุปสรรคที่เกิดขึ้น
- จัดทำรายงานปิดแผนงาน/โครงการ เมื่อดำเนินการแล้วเสร็จ เพื่อประเมินผลสำเร็จของแผนงาน/โครงการ และสรุปสิ่งที่ได้เรียนรู้ (After Action Review) เพื่อเป็นแนวทางการดำเนินงานต่อไปในอนาคต

โดยผู้บริหารด้านเทคโนโลยีสารสนเทศ จะติดตามและประเมินผลการดำเนินงาน เพื่อให้มั่นใจว่า ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ มีการจัดหา/พัฒนาระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม เพื่อให้สามารถบรรลุผลสำเร็จตามตัวชี้วัดของการดำเนินงานภายใต้กรอบเวลาและทรัพยากรที่ได้รับ การจัดสรรไว้

ด้านที่ 4 หลักการด้านผลการดำเนินงาน (Performance)

หลักการ

พิจารณาให้มีการประเมินแผนงานว่า มีความสอดคล้องกับการดำเนินงานและการกำกับดูแลด้านเทคโนโลยีสารสนเทศอย่างไร รวมทั้งประเมินความเสี่ยงที่เกิดจากการจัดการเทคโนโลยีสารสนเทศอย่างสม่ำเสมอเพื่อป้องกันมิให้ทรัพยากรเทคโนโลยีสารสนเทศถูกนำไปใช้อย่างไม่เหมาะสม

แนวปฏิบัติสำหรับผู้รับผิดชอบการกำกับดูแล

ประเมิน (Evaluate)

(1) ผู้รับผิดชอบการกำกับดูแล ประเมินแผนและกิจกรรมด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจได้ว่าเทคโนโลยีสารสนเทศสนับสนุนกระบวนการทางธุรกิจ และในแผนจะต้องระบุกระบวนการปฏิบัติงานและการบริหารจัดการความต่อเนื่องที่ใช้จัดการกับความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม โดยมีขีดความสามารถและสมรรถนะตามที่ต้องการ

(2) ผู้รับผิดชอบการกำกับดูแล ประเมินความเสี่ยงที่เกิดขึ้นจากกิจกรรมด้านเทคโนโลยีสารสนเทศซึ่งมีผลต่อความต่อเนื่องในการดำเนินธุรกิจ รวมถึงความเสี่ยงที่อาจส่งผลกระทบต่อความครบถ้วนถูกต้องของข้อมูล รวมทั้งผลกระทบที่อาจเกิดกับทรัพย์สินสารสนเทศซึ่งรวมถึงข้อมูลสำคัญขององค์กรและประเด็นทรัพย์สินทางปัญญาที่เกี่ยวข้อง

สั่งการ (Direct)

(1) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้มีการจัดสรรทรัพยากรที่เพียงพอเพื่อสนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สามารถตอบสนองความต้องการขององค์กรได้ โดยเป็นไปตามข้อกำหนดด้านงบประมาณและลำดับความสำคัญของงาน โดยมีกระบวนการให้บริการด้านเทคโนโลยีสารสนเทศที่ครอบคลุมการจัดการความมั่นคงปลอดภัยสารสนเทศ การจัดการการเปลี่ยนแปลง การจัดการเหตุขัดข้อง และการบริหารความต่อเนื่องทางธุรกิจอย่างมีประสิทธิภาพด้วย

(2) ผู้รับผิดชอบการกำกับดูแล มอบหมายผู้ที่มีหน้าที่รับผิดชอบในการวางแผน การจัดซื้อ จัดหา จัดจ้าง การติดตั้ง การดำเนินงาน การบริหารจัดการด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจได้ว่าเทคโนโลยีสารสนเทศ สนับสนุนองค์กรตามข้อกำหนดด้านงบประมาณและลำดับความสำคัญของงาน ทั้งนี้ สารสนเทศที่เกี่ยวข้องในการวางแผน การจัดซื้อ จัดหา จัดจ้าง การติดตั้ง การดำเนินงาน การบริหารจัดการด้านเทคโนโลยีสารสนเทศจะต้องมีความถูกต้องและถูกปรับปรุงให้เป็นปัจจุบัน โดยต้องมีมาตรการป้องกันการสูญเสีหรือการนำไปใช้ผิดวัตถุประสงค์อย่างเพียงพอและเหมาะสม

ติดตามผล (Monitor)

(1) ผู้รับผิดชอบการกำกับดูแล ติดตามผลการปฏิบัติตามนโยบายกำกับดูแลด้านเทคโนโลยีสารสนเทศที่ได้วางไว้ รวมทั้งรายงานการติดตามผลได้ถูกนำมาตรวจสอบอย่างถูกต้องและทันเวลา และเพียงพอต่อการนำมาสอบทานโดยผู้ตรวจประเมินทั้งจากภายในและภายนอก

(2) ผู้รับผิดชอบการกำกับดูแล ติดตามผลดำเนินการตามขอบเขตของนโยบายและแนวปฏิบัติต่าง ๆ ด้านเทคโนโลยีสารสนเทศ เช่น ความถูกต้องของข้อมูล และการวางแผน การจัดซื้อ จัดหา จัดจ้าง การติดตั้ง การดำเนินงาน การบริหารจัดการด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีประสิทธิภาพ

แนวปฏิบัติสำหรับผู้บริหารและผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

สำหรับผู้บริหารด้านเทคโนโลยีสารสนเทศ จะประเมินและกำหนดแนวทางการให้บริการด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ สามารถตอบสนองความต้องการของผู้ใช้งาน ซึ่งครอบคลุมถึงการประเมินและบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการให้บริการด้านเทคโนโลยีสารสนเทศ และมีผลกระทบต่อการดำเนินธุรกิจขององค์กร จากนั้นมอบหมายให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศดำเนินการให้บรรลุผลสำเร็จตามแนวทางการให้บริการด้านเทคโนโลยีสารสนเทศที่กำหนดต่อไป ดังนี้

- ดำเนินการบริหารจัดการการร้องขอการบริการ เหตุการณ์ผิดปกติ และปัญหา (Service Request, IT Incident and Problem Management) ตามข้อตกลงการให้บริการด้านเทคโนโลยีสารสนเทศ (Service Level Agreement, SLA) ที่เกี่ยวข้อง
- ดำเนินการบริหารจัดการความต่อเนื่องทางธุรกิจ (BCM) โดยมีการจัดทำแผนรองรับความต่อเนื่องทางธุรกิจ (BCP) รวมถึงมีการซักซ้อมเพื่อให้สามารถบรรลุผลตามวัตถุประสงค์ของแผน BCP เป็นประจำ
- ดำเนินการจัดการคำร้องขอการเปลี่ยนแปลงความต้องการด้านเทคโนโลยีสารสนเทศจากผู้ใช้ (Change Request)
- ดำเนินการบำรุงรักษาระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ โดยมีแผนงานในการบำรุงรักษาที่ชัดเจน
- ดำเนินการตามมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ เช่น มีการกำหนดสิทธิการเข้าใช้งานระบบตามระดับของอำนาจหน้าที่ที่ได้รับมอบหมาย, มีการเก็บ log การใช้งาน และข้อมูล configuration ของระบบเพื่อวิเคราะห์สาเหตุเมื่อเกิดเหตุการณ์ผิดปกติขึ้น
- มีการรายงานผลการให้บริการด้านเทคโนโลยีสารสนเทศ และการประเมินความพึงพอใจของผู้ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำ เพื่อนำผลลัพธ์มาทบทวนปรับปรุงการให้บริการด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพยิ่งขึ้น

โดยผู้บริหารด้านเทคโนโลยีสารสนเทศ จะติดตามและประเมินผลการดำเนินงาน เพื่อให้มั่นใจว่าผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ มีการให้บริการด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ โดยสามารถตอบสนองความคาดหวังและสร้างความพึงพอใจให้แก่ผู้ใช้งานระบบเทคโนโลยีสารสนเทศได้

ด้านที่ 5 หลักการด้านผลความสอดคล้องตามข้อกำหนด (Conformance)

หลักการ

พิจารณาการบริหารจัดการเทคโนโลยีสารสนเทศต้องสอดคล้องตามข้อกำหนดของกฎหมายและระเบียบข้อบังคับทั้งหมดที่มีผลบังคับใช้กับองค์กร ซึ่งรวมถึงนโยบายการกำกับดูแลด้านเทคโนโลยีสารสนเทศ ตลอดจนมีการสื่อสารและบังคับใช้ เพื่อให้เกิดการปฏิบัติในขอบเขตที่เหมาะสม

แนวปฏิบัติสำหรับผู้รับผิดชอบการกำกับดูแล

ประเมิน (Evaluate)

(1) ผู้รับผิดชอบการกำกับดูแล ประเมินขอบข่ายกระบวนการจัดการเทคโนโลยีสารสนเทศว่าเป็นไปตามข้อกำหนดด้านกฎหมาย กฎ ระเบียบ สัญญา/ข้อตกลงต่าง ๆ นโยบายภายใน มาตรฐาน และแนวปฏิบัติในวิชาชีพ

(2) ผู้รับผิดชอบการกำกับดูแล ประเมินผลดำเนินการด้านความสอดคล้องตามข้อกำหนดขององค์กรตามกรอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศ โดยให้มีการประเมินอย่างสม่ำเสมอ

สั่งการ (Direct)

(1) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้ผู้ที่มีหน้าที่รับผิดชอบจัดทำกระบวนการที่ทำให้มั่นใจได้ว่าการจัดการเทคโนโลยีสารสนเทศจะมีความสอดคล้องตามกฎหมาย ระเบียบ นโยบายภายใน มาตรฐาน และแนวทางดำเนินการที่เกี่ยวข้อง

(2) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้มีการจัดทำและประกาศใช้นโยบายต่าง ๆ เพื่อช่วยให้องค์กรบรรลุตามข้อกำหนดต่าง ๆ ในการจัดการเทคโนโลยีสารสนเทศภายในองค์กร และเป็นไปตามหลักมาตรฐานทางจริยธรรมและจรรยาบรรณ

ติดตามผล (Monitor)

(1) ผู้รับผิดชอบการกำกับดูแล ติดตามผลการปฏิบัติตามข้อกำหนดด้านเทคโนโลยีสารสนเทศและผลดำเนินการด้านความสอดคล้องตามข้อกำหนด กฎ ระเบียบต่าง ๆ และมีรูปแบบการรายงานที่ครบถ้วนถูกต้อง เพื่อให้มั่นใจได้ว่าการสอบทานการปฏิบัติตามกฎ ระเบียบ ข้อบังคับเหล่านั้นอย่างสม่ำเสมอและเหมาะสม ครอบคลุมตามกฎ ระเบียบ ข้อบังคับต่าง ๆ ขององค์กร

(2) ผู้รับผิดชอบการกำกับดูแล ติดตามผลดำเนินการในกิจกรรมต่าง ๆ ด้านเทคโนโลยีสารสนเทศเพื่อให้มั่นใจได้ว่าบรรลุผลตามข้อกำหนดต่าง ๆ ทั้งด้านสภาพแวดล้อม การคุ้มครองข้อมูลส่วนบุคคล การจัดการองค์ความรู้เชิงกลยุทธ์ การเก็บรักษาสารสนเทศขององค์กร รวมถึงการทำลายทรัพย์สินสารสนเทศนั้น

แนวปฏิบัติสำหรับผู้บริหารและผู้บริหารงานด้านเทคโนโลยีสารสนเทศ

สำหรับผู้บริหารด้านเทคโนโลยีสารสนเทศ จะประเมินและกำหนดแนวทางการดำเนินงานในด้านความสอดคล้องตามกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ นโยบายต่าง ๆ ด้านเทคโนโลยีสารสนเทศ (อาทิ พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์, พรบ. คุ้มครองข้อมูลส่วนบุคคล) เพื่อให้การดำเนินกิจกรรมด้านเทคโนโลยีสารสนเทศบรรลุผลสำเร็จตามวัตถุประสงค์ของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ นโยบายต่าง ๆ ที่เกี่ยวข้อง และลดความเสี่ยงที่อาจเกิดขึ้น จากนั้นมอบหมายให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศดำเนินการตามแนวทางการดำเนินงานที่กำหนดต่อไป ดังนี้

- ศึกษา ทำความเข้าใจ กฎหมาย ระเบียบ คำสั่ง ข้อบังคับ นโยบายต่าง ๆ ที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ
- ดำเนินการให้สอดคล้องตามกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ นโยบายต่าง ๆ ด้านเทคโนโลยีสารสนเทศ ทั้งภายในและภายนอกที่เกี่ยวข้อง ในทุกขั้นตอนของการดำเนินงานด้านเทคโนโลยีสารสนเทศ ครอบคลุมตั้งแต่ การเริ่มจัดทำแผนงาน/โครงการ การจัดซื้อจัดจ้าง การออกแบบ การพัฒนา ไปจนถึงการนำระบบเทคโนโลยีสารสนเทศออกให้บริการ

โดยผู้บริหารด้านเทคโนโลยีสารสนเทศ จะติดตามและประเมินผลการดำเนินงาน เพื่อให้มั่นใจว่าผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศสามารถดำเนินงานให้บรรลุผลสำเร็จ โดยมีการปฏิบัติตามกฎหมาย ระเบียบ คำสั่ง ข้อบังคับต่าง ๆ ด้านเทคโนโลยีสารสนเทศอย่างถูกต้องและเหมาะสม

ด้านที่ 6 หลักการด้านพฤติกรรมบุคคล (Human Behavior)

หลักการ

พิจารณากำหนดนโยบาย แนวปฏิบัติ และกิจกรรมด้านเทคโนโลยีสารสนเทศ โดยคำนึงถึงความสามารถในการนำไปปรับใช้ในทางปฏิบัติได้จริงกับบุคลากร ทั้งยังต้องคำนึงถึงความต้องการ ข้อจำกัด และแนวทางการพัฒนาสำหรับบุคลากรในกระบวนการทั้งหมดด้วย

แนวปฏิบัติสำหรับผู้รับผิดชอบการกำกับดูแล

ประเมิน (Evaluate)

(1) ผู้รับผิดชอบการกำกับดูแล ประเมินทรัพยากรและกิจกรรมด้านเทคโนโลยีสารสนเทศ ให้สอดคล้องกัน เพื่อให้มั่นใจได้ว่าแนวทางการปฏิบัติของบุคลากร ได้ถูกกำหนดและสื่อสารเพื่อทำความเข้าใจอย่างเหมาะสม

(2) ผู้รับผิดชอบการกำกับดูแล ประเมินขีดความสามารถ ความรู้ความเข้าใจของบุคลากร ต่อการใช้งานเทคโนโลยีสารสนเทศเพื่อวางแผนพัฒนาความรู้ของบุคลากร

สั่งการ (Direct)

(1) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้ผู้มีหน้าที่รับผิดชอบ กำหนดกิจกรรมที่เกี่ยวข้องกับการใช้งานหรือการให้บริการด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแนวทางการปฏิบัติของบุคลากรที่กำหนดไว้

(2) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้มีการกำหนดผู้รับผิดชอบและกรอบระยะเวลาในการรายงานหากเกิดประเด็นเกี่ยวกับความเสี่ยง โอกาสทางธุรกิจ ปัญหา โดยประเด็นเหล่านี้จะต้องได้รับการบริหารจัดการให้สอดคล้องกับนโยบายและแนวปฏิบัติที่ประกาศใช้ ตลอดจนการนำเสนอประเด็นสำคัญไปยังผู้มีอำนาจตัดสินใจ

ติดตามผล (Monitor)

(1) ผู้รับผิดชอบการกำกับดูแล ติดตามผลดำเนินการตามกิจกรรมด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจได้ว่าแนวทางการปฏิบัติของบุคลากรได้รับการติดตามตรวจสอบอย่างสม่ำเสมอ และยังคงเป็นไปตามแนวทางที่กำหนด

(2) ผู้รับผิดชอบการกำกับดูแล ติดตามผลดำเนินการตามวิธีปฏิบัติงาน เพื่อให้มั่นใจได้ว่าวิธีปฏิบัติงานนั้นมีความเหมาะสมและสอดคล้องกับการจัดการเทคโนโลยีสารสนเทศและนโยบายการกำกับดูแลด้านเทคโนโลยีสารสนเทศ

แนวปฏิบัติสำหรับผู้บริหารและผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

สำหรับผู้บริหารด้านเทคโนโลยีสารสนเทศ จะประเมินและกำหนดแนวทางที่จะส่งเสริมให้บุคลากรในองค์กรมีความรู้ความสามารถในการดำเนินงานในส่วนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ จากนั้นมอบหมายให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศดำเนินการตามแนวทางการดำเนินงานที่กำหนดต่อไป ดังนี้

- จัดให้มีการฝึกอบรมเพื่อเพิ่มขีดความสามารถของบุคลากรด้านเทคโนโลยีสารสนเทศ ซึ่งมีหน้าที่ในการพัฒนาและให้บริการระบบงานด้านเทคโนโลยีสารสนเทศให้ตรงตามความต้องการของผู้ใช้ และบุคลากรทั่วไป ที่ต้องสามารถใช้บริการด้านเทคโนโลยีสารสนเทศ

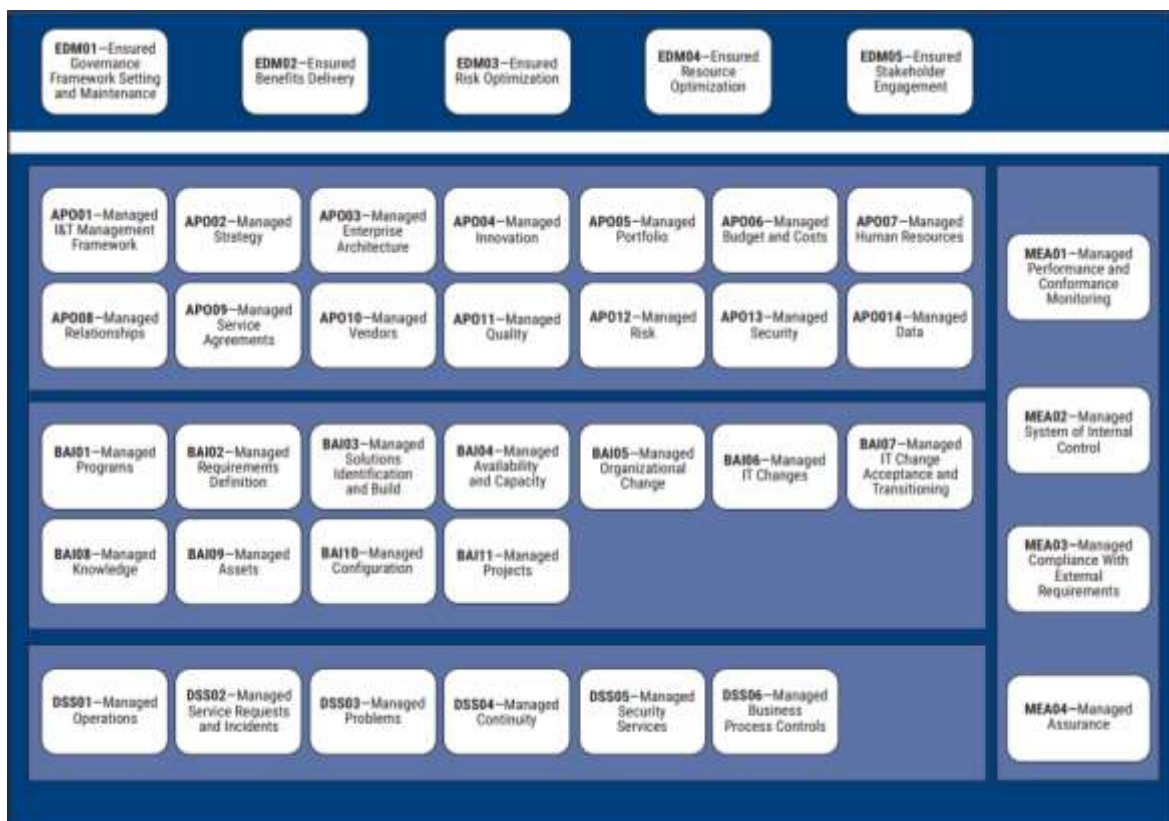
ที่องค์กรพัฒนาขึ้น เพื่อเพิ่มประสิทธิภาพการดำเนินงานตามหน้าที่ความรับผิดชอบได้อย่างมีประสิทธิภาพ

- บริหารการเปลี่ยนแปลงตลอดทุกขั้นตอนของการดำเนินงานด้านเทคโนโลยีสารสนเทศ เพื่อให้ผู้มีส่วนได้ส่วนเสียยอมรับการเปลี่ยนแปลงในด้านต่าง ๆ ที่เกิดขึ้น และสนับสนุนให้แผนงาน/โครงการด้านเทคโนโลยีสารสนเทศบรรลุผลสำเร็จ และมีการสื่อสาร ประชาสัมพันธ์ ผูกอบรวม และประเมินประสิทธิผล เพื่อสร้างความตระหนัก ความรู้ ความเข้าใจแก่ผู้มีส่วนได้ส่วนเสีย

โดยผู้บริหารด้านเทคโนโลยีสารสนเทศ จะติดตามและประเมินผลการดำเนินงาน เพื่อให้มั่นใจว่าผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ สามารถดำเนินการสร้างความตระหนัก ความรู้ ความเข้าใจ เพื่อให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ สนับสนุนให้การดำเนินงานด้านเทคโนโลยีสารสนเทศบรรลุผลสำเร็จตามวัตถุประสงค์

6.2 แนวปฏิบัติที่ดีในการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ

เพื่อให้การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศดำเนินไปอย่างเป็นระบบและมีประสิทธิภาพ สามารถสนับสนุนการนำนโยบายการกำกับดูแลด้านเทคโนโลยีสารสนเทศไปสู่การปฏิบัติให้เกิดผลลัพธ์ (Outcome) ที่ดีขึ้นอย่างต่อเนื่อง จึงได้มีการนำกรอบการดำเนินงานด้านการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร (COBIT 2019) ซึ่งประกอบด้วย 40 กระบวนการที่ครอบคลุมการดำเนินงานต่าง ๆ ด้านเทคโนโลยีสารสนเทศในองค์กร มาประยุกต์ใช้เป็นแนวปฏิบัติที่ดีในการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ



7. ภาคผนวก

7.1 มาตรฐานและแนวปฏิบัติอ้างอิง

- ISO/IEC 38500 (Governance of IT for the organization) มาตรฐานสากลว่าด้วยการกำกับดูแลด้านเทคโนโลยีสารสนเทศสำหรับองค์กร
- COBIT 2019 (A Business Framework for the Governance and Management of Enterprise IT) แนวปฏิบัติที่ดีสำหรับการดำเนินงานในการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศขององค์กร