การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

แนวปฏิบัติประกอบนโยบาย การกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ (IT Governance Procedure)

รหัสเอกสาร : ITG-SD-001
เวอร์ชัน : 1.1

สำนักดิจิทัล **ฝ่ายกลยุทธ์ดิจิทัลและบริหารจัดการข้อมูล** **กองกลยุทธ์ดิจิทัล**	**อนุมัติ** (ลงชื่อ)..... (.....ว่าที่ ร.ท. สมพงษ์ สมันเลาะ.....) ตำแหน่ง.....รองผู้ว่าการสารสนเทศและสื่อสาร..... -/ 1 เม.ย. 2564 A-WM-01

ประวัติการปรับปรุงเอกสาร

เวอร์ชัน	วันที่มีผลบังคับใช้	ผู้ดำเนินการ	รายละเอียด
1.0	29 ธ.ค. 2563	กดท.	ออกเอกสารครั้งแรก
1.1	1 เม.ย. 2564	กดท.	ทบทวนครั้งที่ 1 ปรับปรุงเพิ่มเติมตามผลการตรวจสอบภายใน ITG (ITG Internal Audit) ปี 2564 - ความถี่ในการทบทวนเอกสาร - ขยายความเพิ่มเติมในหมวด 2-4 เพื่อให้มั่นใจได้ว่ากระบวนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศครอบคลุมถึงด้าน ความมั่นคงปลอดภัยสารสนเทศ การจัดการการเปลี่ยนแปลง การจัดการเหตุขัดข้อง และการบริหารความเนื่องทางธุรกิจ

สารบัญ

หน้า

1. บทนำ

การไฟฟ้าส่วนภูมิภาคตระหนักถึงความสำคัญในการใช้เทคโนโลยีสารสนเทศให้มีประสิทธิผล ประสิทธิภาพ และเป็นที่ยอมรับ ตอบสนองความต้องการของผู้มีส่วนได้ส่วนเสียในการดำเนินธุรกิจและภารกิจของการไฟฟ้าส่วนภูมิภาค มีการกำกับดูแล การบริหารจัดการที่ดีด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่องตามหลักการกำกับดูแลกิจการที่ดี รวมทั้งมีการบริหารจัดการที่ดีเลิศและบูรณาการตามแนวทางการกำกับดูแลการบริหารความเสี่ยง และการปฏิบัติตามกฎเกณฑ์ (Integrated GRC: Governance, Risk Management and Compliance)

ปัจจุบัน การไฟฟ้าส่วนภูมิภาคได้นำหลักการและแนวทางการปฏิบัติตามมาตรฐานสากลและแนวปฏิบัติที่ดีเลิศ (Standards and Best Practices) ได้แก่ มาตรฐาน ISO/IEC 38500 (Governance of IT for the Organization) และ COBIT 5 (A Business Framework for the Governance and Management of Enterprise IT) มาใช้ในการกำกับดูแลและการบริหารจัดการด้านเทคโนโลยีสารสนเทศ ที่มีการกำหนดทิศทางและควบคุม โดยมีการประเมิน (Evaluate) สั่งการ (Direct) และติดตามผล (Monitor) สำหรับการจัดการเทคโนโลยีสารสนเทศทั้งในปัจจุบันและอนาคต ตั้งแต่การวางแผน ออกแบบ พัฒนา ติดตั้งใช้งาน ปฏิบัติงาน บริหารจัดการ และประยุกต์ใช้เทคโนโลยีสารสนเทศ โดยการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศของการไฟฟ้าส่วนภูมิภาค ได้ยึดหลักการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ (Principles for Good Governance of IT) ตามมาตรฐานสากล ISO/IEC 38500 (Governance of IT for the Organization) ดังนี้

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

การกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ (IT Governance, ITG) อย่างเป็นระบบ จะเป็นกลไกสำคัญในการสนับสนุนการกำกับดูแลกิจการที่ดี (Corporate Governance) ทั้งในเรื่องของการกำหนดนโยบาย มาตรฐาน และแนวปฏิบัติ เพื่อสร้างความเชื่อมั่นในการให้บริการด้านเทคโนโลยีสารสนเทศ การจัดการความเสี่ยง และการสร้างโอกาสทางธุรกิจจากการนำระบบเทคโนโลยีสารสนเทศมาใช้ รวมไปถึงเรื่องของการปฏิบัติงานที่สอดคล้องกับกฎหมาย ข้อบังคับ กฎ ระเบียบ และข้อกำหนดต่าง ๆ อันจะเป็นการสร้างคุณค่าจากการใช้งานเทคโนโลยีสารสนเทศ ตลอดจนสนับสนุนการดำเนินงานตามแผนงานและยุทธศาสตร์การไฟฟ้าส่วนภูมิภาคให้เป็นไปอย่างมีประสิทธิภาพ

2. วัตถุประสงค์

เพื่อให้การไฟฟ้าส่วนภูมิภาคมีการกำกับดูแลและการบริหารจัดการด้านเทคโนโลยีสารสนเทศ ที่สอดคล้องตามมาตรฐานสากลและแนวปฏิบัติที่ดีเลิศ มีแนวทางการปฏิบัติให้ผู้บริหาร พนักงาน ลูกจ้าง และผู้ปฏิบัติงานให้กับการไฟฟ้าส่วนภูมิภาค ได้รับทราบและยึดถือปฏิบัติในการดำเนินการที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ อันจะเป็นการดำรงไว้ซึ่งการกำกับดูแลและบริหารจัดการที่ดีด้านเทคโนโลยีสารสนเทศของการไฟฟ้าส่วนภูมิภาค

3. ขอบเขต

นโยบายฉบับนี้ครอบคลุมแนวทางการปฏิบัติสำหรับผู้บริหาร พนักงาน ลูกจ้าง และผู้ปฏิบัติงานให้กับการไฟฟ้าส่วนภูมิภาค 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 หรือรับรู้ว่าพวกเขาได้รับผลกระทบจากการตัดสินใจหรือกิจกรรมของการไฟฟ้าส่วนภูมิภาค ได้แก่ หน่วยงานกำกับดูแล พนักงาน ผู้ส่งมอบ คู่ค้า คู่ความร่วมมือ ลูกค้า/ผู้ใช้บริการ และชุมชน สังคม และสิ่งแวดล้อม

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

3. “การกำกับดูแล” (Governance) หมายความว่า การกำหนดนโยบาย การติดตามผลการดำเนินการอย่างต่อเนื่องโดยผู้รับผิดชอบการกำกับดูแล

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

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

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

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

7. “การบริหารจัดการ” (Management) หมายความว่า การดำเนินการในการควบคุม (control) และ ควบคุมดูแล (supervision) ภายใต้อำนาจหน้าที่และภาระรับผิดชอบที่กำหนดขึ้นจากการกำกับดูแล (governance) เพื่อให้บรรลุวัตถุประสงค์ขององค์กร การบริหารจัดการให้มีประสิทธิภาพและประสิทธิผล ประกอบด้วย

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

8. “ภาระรับผิดชอบ” (Accountability) หมายความว่า สถานะของการมีภาระรับผิดชอบต่อผลสัมฤทธิ์หรือความสำเร็จของงาน

9. “หน้าที่รับผิดชอบ” (Responsibility) หมายความว่า พันธะผูกพันที่จะต้องดำเนินการและตัดสินใจเพื่อให้บรรลุผลลัพธ์ที่ต้องการ ความรับผิดชอบต่อการปฏิบัติงานตามหน้าที่หรือตามที่รับมอบหมาย ให้บรรลุผลตามที่กำหนด

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

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

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

13. “ปัจจัยภายใน” หมายความว่า ปัจจัยขับเคลื่อนหรือบริบทภายในองค์กร สภาพแวดล้อมภายในองค์กรที่มีผลต่อการบรรลุวัตถุประสงค์ขององค์กร 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

14. “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

15. “ทรัพย์สินสารสนเทศ” หมายความว่า สินทรัพย์/ทรัพย์สิน ที่เป็นระบบและอุปกรณ์ประเภทซอฟต์แวร์ ฮาร์ดแวร์ ข้อมูลและสารสนเทศ ทั้งที่อยู่ในรูปอิเล็กทรอนิกส์ เอกสาร และข้อความเสียง โดยประกอบด้วย

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

5. การดำเนินการตามนโยบายการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ

การไฟฟ้าส่วนภูมิภาคได้กำหนดนโยบายการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ และมีแนวทางการดำเนินการตามนโยบายฯ ดังต่อไปนี้

1. กำหนดให้มีโครงสร้างการกำกับดูแลที่ดีด้านเทคโนโลยีสารสารสนเทศ พร้อมทั้งกำหนดบทบาทและหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง
2. กำหนดให้มีการจัดทำแนวทางหรือขั้นตอนปฏิบัติเพื่อกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศให้เป็นไปตามมาตรฐานสากล ISO/IEC 38500 (Governance of IT for the Organization)
3. กำหนดแนวทางและส่งเสริมให้หน่วยงานที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ ปฏิบัติตามแนวทางหรือขั้นตอนการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศของการไฟฟ้าส่วนภูมิภาค
4. กำหนดให้มีการติดตามผลการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศอยู่เสมอ และรายงานให้คณะกรรมการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ (IT Governance Committee) อยู่เสมอเพื่อพิจารณาให้ข้อคิดเห็น
5. กำหนดให้มีการตรวจสอบ การตรวจติดตามการนำไปปฏิบัติตามนโยบาย แนวปฏิบัติ และกระบวนการโดยให้ความเป็นอิสระในการตรวจสอบ รายงานให้คณะกรรมการ กฟภ. อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง เพื่อพิจารณาให้ข้อคิดเห็น
6. กำหนดให้มีการทบทวน นโยบายการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ แนวปฏิบัติประกอบนโยบายฯ บริบทการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ คู่มือการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ ข้อกำหนดสำหรับผลลัพธ์ เกณฑ์วัด และวิธีการประเมินระบบการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ (ITG Beneficial Outcomes) และเอกสารที่เกี่ยวข้องอย่างน้อยปีละ 1 ครั้ง

6. แนวทางดำเนินงาน ตาม Model for Good Governance of IT และ Principles for Good Governance of IT ตามมาตรฐาน ISO/IEC 38500

ผู้รับผิดชอบการกำกับดูแล (Governing Bodies) ด้านเทคโนโลยีสารสนเทศของการไฟฟ้าส่วนภูมิภาคต้องดำเนินการตามหลักการ 6 หมวด ดังนี้

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

หมวด 1 หลักการด้านความรับผิดชอบ (Responsibility)

<u>หลักการ</u>

พิจารณาแต่งตั้งให้มีบุคคลที่มีหน้ารับผิดชอบเพื่อจัดการความต้องการในการใช้เทคโนโลยีสารสนเทศ และจัดให้มีบริการที่จำเป็นตามความต้องการนั้นทั้งในปัจจุบันและอนาคต โดยต้องมีการกำหนดอำนาจหน้าที่ในการดำเนินงานอย่างเหมาะสม เป็นไปตามแนวทางเดียวกันกับยุทธศาสตร์องค์กร

แนวปฏิบัติ

1.1 ประเมิน (Evaluate)

(1) ผู้รับผิดชอบการกำกับดูแล กำหนดให้มีกฎบัตร หรือคำบรรยายลักษณะงาน (Job Description) ของผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศ ให้มั่นใจได้ว่าการจัดการเทคโนโลยีสารสนเทศภายในองค์กรเกิดประสิทธิภาพ ประสิทธิผล รวมทั้งสนับสนุนวัตถุประสงค์การดำเนินงานของการไฟฟ้าส่วนภูมิภาคทั้งในปัจจุบันและอนาคต

(2) ผู้รับผิดชอบการกำกับดูแล ประเมินความสามารถของผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

1.2 สั่งการ (Direct)

(1) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้ผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศปฏิบัติหน้าที่ตามยุทธศาสตร์ของการไฟฟ้าส่วนภูมิภาค

(2) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้ผู้มีหน้าที่รับผิดชอบด้านเทคโนโลยีสารสนเทศต้องได้รับข้อมูลที่จำเป็นในการปฏิบัติงานเพื่อให้บรรลุเป้าหมายที่วางไว้ โดยผู้รับผิดชอบการกำกับดูแลให้สิทธิแก่ผู้มีหน้าที่รับผิดชอบด้านเทคโนโลยีสารสนเทศในการเข้าถึงข้อมูลที่จำเป็น หรือมอบหมายหน้าที่ในการสนับสนุนข้อมูลที่จำเป็นแก่ผู้มีหน้าที่รับผิดชอบด้านเทคโนโลยีสารสนเทศท่านอื่น

1.3 ติดตามผล (Monitor)

(1) ผู้รับผิดชอบการกำกับดูแล ติดตาม ประเมินความเหมาะสมของการกำหนดโครงสร้าง และการแบ่งแยกหน้าที่ว่ามีความเหมาะสมหรือไม่ รวมทั้งผลการดำเนินงานของผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศ นอกจากนี้ควรประเมินความเข้าใจในบทบาทหน้าที่และความรับผิดชอบของผู้ได้รับมอบหมายด้วย

(2) ผู้รับผิดชอบการกำกับดูแล ติดตามผลการดำเนินงานของผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศ รวมถึงความสามารถในการปฏิบัติงานและเสนอแผนงานที่เป็นประโยชน์เพื่อส่งเสริมการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการผู้รับผิดชอบการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ

หมวด 2 หลักการด้านยุทธศาสตร์ (Strategy)

<u>หลักการ</u>

พิจารณาถึงขีดความสามารถและแผนงานด้านเทคโนโลยีสารสนเทศ ทั้งในปัจจุบันและอนาคต เพื่อตอบสนองความต้องการตามยุทธศาสตร์ขององค์กร

<u>แนวปฏิบัติ</u>

2.1 ประเมิน (Evaluate)

(1) ผู้รับผิดชอบการกำกับดูแล ประเมินการพัฒนาด้านเทคโนโลยีสารสนเทศ และกระบวนการทำงานขององค์กร เพื่อให้มั่นใจได้ว่ามีความสอดคล้องและสนับสนุนแผนงานของการไฟฟ้าส่วนภูมิภาคทั้งในปัจจุบันและในอนาคต

(2) ผู้รับผิดชอบการกำกับดูแล ประเมินการจัดการเทคโนโลยีสารสนเทศและกิจกรรมด้านเทคโนโลยีสารสนเทศ ซึ่งเป็นส่วนหนึ่งในการจัดทำแผนงานและนโยบาย เพื่อให้มั่นใจได้ว่าการดำเนินการเกี่ยวกับเทคโนโลยีสารสนเทศนั้นสอดคล้องเป็นไปในแนวทางเดียวกับวัตถุประสงค์ขององค์กรและอยู่ในระดับความเสี่ยงที่เหมาะสม รวมทั้งตอบสนองต่อความต้องการหลักของผู้มีส่วนได้ส่วนเสียที่แท้จริง ทั้งนี้ให้นำแนวปฏิบัติที่ดีมาใช้ในการปฏิบัติงานจริงด้วย

2.2 สั่งการ (Direct)

(1) ผู้รับผิดชอบการกำกับดูแล มอบหมาย สั่งการให้มีการพัฒนาด้านเทคโนโลยีสารสนเทศ โดยต้องสอดคล้องกับยุทธศาสตร์และแผนปฏิบัติการดิจิทัล ตลอดจนการนำแผนปฏิบัติการดิจิทัลไปใช้ในการปฏิบัติงานจริง โดยครอบคลุมถึงการวางแผนเพื่อให้มีการจัดการความมั่นคงปลอดภัยสารสนเทศ การจัดการการเปลี่ยนแปลง การจัดการเหตุขัดข้อง และการบริหารความเนื่องทางธุรกิจอย่างมีประสิทธิภาพ เพื่อให้มั่นใจได้ว่าองค์กรได้รับประโยชน์สูงสุดจากการพัฒนาด้านเทคโนโลยีสารสนเทศ

(2) ผู้รับผิดชอบการกำกับดูแล ส่งเสริมให้ผู้มีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีสารสนเทศนำเสนอข้อเสนอแผนงานการพัฒนาด้านเทคโนโลยีสารสารสนเทศ เพื่อให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยี ซึ่งจะช่วยให้องค์กรสามารถตอบสนองต่อความท้าทาย และเพิ่มโอกาสในการแข่งขันทางธุรกิจ

2.3 ติดตามผล (Monitor)

(1) ผู้รับผิดชอบการกำกับดูแล ติดตามผลของการจัดการเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าองค์กรได้รับประโยชน์ตามเป้าหมายที่กำหนดไว้ในข้อเสนอแผนงาน

(2) ผู้รับผิดชอบการกำกับดูแล ติดตามสถานะความคืบหน้าของข้อเสนอแผนงานด้านเทคโนโลยีสารสนเทศตามที่ได้รับอนุมัติอย่างต่อเนื่อง เพื่อให้มั่นใจได้ว่าข้อเสนอแผนงานนั้นได้ดำเนินการตามวัตถุประสงค์ภายใต้กรอบเวลาและทรัพยากรตามที่ได้รับจัดสรรไว้อย่างเหมาะสม

หมวด 3 หลักการด้านการจัดหา (Acquisition)

<u>หลักการ</u>

พิจารณาให้มีการจัดหาเทคโนโลยีสารสนเทศอย่างสมเหตุสมผล บนพื้นฐานของการวิเคราะห์อย่างเหมาะสมและต่อเนื่อง ด้วยการตัดสินใจที่ชัดเจนและโปร่งใส มีความสมดุลที่เหมาะสมระหว่างประโยชน์ที่ได้รับ โอกาสทางธุรกิจ ค่าใช้จ่าย และความเสี่ยง ทั้งในระยะสั้นและระยะยาว

<u>แนวปฏิบัติ</u>

3.1 ประเมิน (Evaluate)

(1) ผู้รับผิดชอบการกำกับดูแล ประเมินทางเลือกสำหรับการจัดซื้อ จัดหา จัดจ้างเทคโนโลยีสารสนเทศ ตามข้อเสนอแผนงานที่ได้รับอนุมัติ โดยพิจารณาถึงความเหมาะสมถึงความเสี่ยงและความคุ้มค่าจากการลงทุน

3.2 สั่งการ (Direct)

(1) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้ผู้รับผิดชอบจัดหาทรัพย์สินสารสนเทศที่จำเป็นอย่างเหมาะสม รวมถึงกำหนดแนวทางหรือวิธีปฏิบัติในการจัดหาเป็นลายลักษณ์อักษร

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

3.3 ติดตามผล (Monitor)

(1) ผู้รับผิดชอบการกำกับดูแล ติดตามผลดำเนินงานที่ได้มีการลงทุนด้านเทคโนโลยีสารสนเทศเพื่อให้มั่นใจได้ว่าผลลัพธ์เป็นไปตามดัชนีชี้วัดและเกิดประโยชน์ตามที่ผู้มีส่วนได้ส่วนเสียคาดหวัง

(2) ผู้รับผิดชอบการกำกับดูแล ติดตามขอบเขตของการสื่อสารและทำความเข้าใจที่เกิดขึ้นระหว่างบุคคลที่เกี่ยวข้องในองค์กรและผู้ให้บริการภายนอก

หมวด 4 หลักการด้านผลการดำเนินงาน (Performance)

<u>หลักการ</u>

พิจารณาให้มีการประเมินแผนงานว่า มีความสอดคล้องกับการดำเนินงานและการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศอย่างไร รวมทั้งประเมินความเสี่ยงที่เกิดจากการจัดการเทคโนโลยีสารสนเทศอย่างสม่ำเสมอเพื่อป้องกันมิให้ทรัพยากรเทคโนโลยีสารสนเทศถูกนำไปใช้อย่างไม่เหมาะสม

<u>แนวปฏิบัติ</u>

4.1 ประเมิน (Evaluate)

(1) ผู้รับผิดชอบการกำกับดูแล ประเมินแผนและกิจกรรมด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจได้ว่าเทคโนโลยีสารสนเทศสนับสนุนกระบวนการทางธุรกิจ และในแผนจะต้องระบุกระบวนการปฏิบัติงานและการบริหารจัดการความต่อเนื่องที่ใช้จัดการกับความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม โดยมีขีดความสามารถและสมรรถนะตามที่ต้องการ

(2) ผู้รับผิดชอบการกำกับดูแล ประเมินความเสี่ยงที่เกิดขึ้นจากกิจกรรมด้านเทคโนโลยีสารสนเทศซึ่งมีผลต่อความต่อเนื่องในการดำเนินธุรกิจ รวมถึงความเสี่ยงที่อาจส่งผลต่อความครบถ้วนถูกต้องของข้อมูล รวมทั้งผลกระทบที่อาจเกิดกับทรัพย์สินสารสนเทศซึ่งรวมถึงข้อมูลสำคัญขององค์กรและประเด็นทรัพย์สินทางปัญญาที่เกี่ยวข้อง

4.2 สั่งการ (Direct)

(1) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้มีการจัดสรรทรัพยากรที่เพียงพอเพื่อสนับสนุนการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สามารถตอบสนองความต้องการขององค์กรได้ โดยเป็นไปตามข้อจำกัดด้านงบประมาณและลำดับความสำคัญของงาน โดยมีกระบวนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศอย่างน้อยครอบคลุมด้านความมั่นคงปลอดภัยสารสนเทศ การจัดการการเปลี่ยนแปลง การจัดการเหตุขัดข้อง และการบริหารความเนื่องทางธุรกิจ

(2) ผู้รับผิดชอบการกำกับดูแล มอบหมายผู้ที่มีหน้าที่รับผิดชอบในการวางแผน การจัดซื้อ จัดหา จัดจ้าง การติดตั้ง การดำเนินงาน การบริหารจัดการด้านเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจได้ว่าเทคโนโลยีสารสนเทศ สนับสนุนองค์กรตามข้อจำกัดด้านงบประมาณและลำดับความสำคัญของงาน ทั้งนี้ สารสนเทศที่เกี่ยวข้องในการวางแผน การจัดซื้อ จัดหา จัดจ้าง การติดตั้ง การดำเนินงาน การบริหารจัดการด้านเทคโนโลยีสารสนเทศจะต้องมีความถูกต้องและถูกปรับปรุงให้เป็นปัจจุบัน โดยต้องมีมาตรการป้องกันการสูญเสียหรือการนำไปใช้ผิดวัตถุประสงค์อย่างเพียงพอและเหมาะสม

4.3 ติดตามผล (Monitor)

(1) ผู้รับผิดชอบการกำกับดูแล ติดตามผลการปฏิบัติตามนโยบายกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศที่ได้วางไว้ รวมทั้งรายงานการติดตามผลได้ถูกนำมาตรวจสอบอย่างถูกต้องและทันเวลา และเพียงพอต่อการนำมาสอบทานโดยผู้ตรวจสอบทั้งจากภายในและภายนอก

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

หมวด 5 หลักการด้านผลความสอดคล้องตามข้อกำหนด (Conformance)

หลักการ

พิจารณาการบริหารจัดการเทคโนโลยีสารสนเทศต้องสอดคล้องตามข้อกำหนดของกฎหมายและระเบียบข้อบังคับทั้งหมดที่มีผลบังคับใช้กับองค์กร ซึ่งรวมถึงนโยบายการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ ตลอดจนมีการสื่อสารและบังคับใช้ เพื่อให้เกิดการปฏิบัติในขอบเขตที่เหมาะสม

แนวปฏิบัติ

5.1 ประเมิน (Evaluate)

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

(2) ผู้รับผิดชอบการกำกับดูแล ประเมินผลดำเนินการด้านความสอดคล้องตามข้อกำหนดขององค์กรตามกรอบการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ โดยให้มีการประเมินอย่างสม่ำเสมอ

5.2 สั่งการ (Direct)

(1) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้ผู้ที่มีหน้าที่รับผิดชอบจัดทำกระบวนการที่ทำให้มั่นใจได้ว่า การจัดการเทคโนโลยีสารสนเทศจะมีความสอดคล้องตามกฎระเบียบ นโยบายภายใน มาตรฐาน และแนวทางดำเนินการที่เกี่ยวข้อง

(2) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้มีการจัดทำและประกาศใช้นโยบายต่าง ๆ เพื่อช่วยให้องค์กรบรรลุตามข้อกำหนดต่าง ๆ ในการจัดการเทคโนโลยีสารสนเทศภายในองค์กร และเป็นไปตามหลักมาตรฐานทางจริยธรรมและจรรยาบรรณ

5.3 ติดตามผล (Monitor)

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

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

หมวด 6 หลักการด้านพฤติกรรมบุคคล (Human Behavior)

<u>หลักการ</u>

พิจารณากำหนดนโยบาย แนวปฏิบัติ และกิจกรรมด้านเทคโนโลยีสารสนเทศ โดยคำนึงถึงความสามารถในการนำไปปรับใช้ในทางปฏิบัติได้จริงกับบุคลากร ทั้งยังต้องคำนึงถึงความต้องการ ข้อจำกัด และแนวทางการพัฒนาสำหรับบุคลากรในกระบวนการทั้งหมดด้วย

<u>แนวปฏิบัติ</u>

6.1 ประเมิน (Evaluate)

(1) ผู้รับผิดชอบการกำกับดูแล ประเมินทรัพยากรและกิจกรรมด้านเทคโนโลยีสารสนเทศให้สอดคล้องกัน เพื่อให้มั่นใจได้ว่าแนวทางการปฏิบัติของบุคลากร ได้ถูกกำหนดและสื่อสารเพื่อทำความเข้าใจอย่างเหมาะสม

(2) ผู้รับผิดชอบการกำกับดูแล ประเมินขีดความสามารถ ความรู้ความเข้าใจของบุคลากร ต่อการใช้งานเทคโนโลยีสารสนเทศเพื่อวางแผนพัฒนาความรู้ของบุคลากร

6.2 สั่งการ (Direct)

(1) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้ผู้มีหน้าที่รับผิดชอบ กำหนดกิจกรรมที่เกี่ยวข้องกับการใช้งานหรือการให้บริการด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแนวทางการปฏิบัติของบุคลากรที่กำหนดไว้

(2) ผู้รับผิดชอบการกำกับดูแล มอบหมายให้มีการกำหนดผู้รับผิดชอบและกรอบระยะเวลาในการรายงานหากเกิดประเด็นเกี่ยวกับความเสี่ยง โอกาสทางธุรกิจ ปัญหา โดยประเด็นเหล่านี้จะต้องได้รับการบริหารจัดการให้สอดคล้องกับนโยบายและแนวปฏิบัติที่ประกาศใช้ ตลอดจนการนำเสนอประเด็นสำคัญไปยังผู้มีอำนาจตัดสินใจ

6.3 ติดตามผล (Monitor)

(1) ผู้รับผิดชอบการกำกับดูแล ติดตามผลดำเนินการตามกิจกรรมด้านเทคโนโลยีสารสนเทศเพื่อให้มั่นใจได้ว่าแนวทางการปฏิบัติของบุคลากรได้รับการติดตามตรวจสอบอย่างสม่ำเสมอ และยังคงเป็นไปตามแนวทางที่กำหนด

(2) ผู้รับผิดชอบการกำกับดูแล ติดตามผลดำเนินการตามวิธีปฏิบัติงาน เพื่อให้มั่นใจได้ว่าวิธีปฏิบัติงานนั้นมีความเหมาะสมและสอดคล้องกับการจัดการเทคโนโลยีสารสนเทศและนโยบายการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ

7. มาตรฐานและแนวปฏิบัติอ้างอิง

ISO/IEC 38500 (Governance of IT for the organization) มาตรฐานสากลว่าด้วยการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศสำหรับองค์กร