ประกาศการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย
เรื่อง นโยบายความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

โดยที่เห็นสมควรปรับปรุงประกาศ เรื่อง นโยบายความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ เนื่องจากมีการปรับปรุงนโยบายการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของ กฟผ. เป็นไปอย่างมีประสิทธิภาพ สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ตลอดจนเกณฑ์การประเมินผลการดำเนินการรัฐวิสาหกิจด้านการพัฒนาเทคโนโลยีดิจิทัลของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ผู้ว่าการการไฟฟ้าฝ่ายผลิตแห่งประเทศไทยออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้ยกเลิกประกาศการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย ที่ ๔๒/๒๕๖๕ เรื่อง นโยบายความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

ข้อ ๒ หน่วยงานสำคัญซึ่งปฏิบัติภารกิจหลักของ กฟผ. และหน่วยงานโครงสร้างพื้นฐานด้านเทคโนโลยีปฏิบัติการและเทคโนโลยีดิจิทัลของ กฟผ. ได้แก่ โรงไฟฟ้า ศูนย์ควบคุมระบบกำลังไฟฟ้า ศูนย์ปฏิบัติการภาคสถานีไฟฟ้า โครงข่ายระบบสื่อสาร การให้บริการเทคโนโลยีปฏิบัติการและเทคโนโลยีดิจิทัล มีหน้าที่ดำเนินการควบคุมและกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

ข้อ ๓ ให้หน่วยงานตามข้อ ๒ ดำเนินการตามประมวลแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ดังต่อไปนี้

(๑) เข้ารับการตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศโดยผู้ตรวจสอบภายในอย่างน้อยปีละ ๑ ครั้ง ตามแผนการตรวจสอบประจำปีของสำนักงานตรวจสอบภายใน

(๒) ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

(๓) ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์และสารสนเทศ และฝึกซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์และสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔ ให้หน่วยงานตามข้อ ๒ ดำเนินการตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ดังต่อไปนี้

(๑) ระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify) โดยครอบคลุมในเรื่อง ดังต่อไปนี้

(๑.๑) การจัดการทรัพย์สิน (Asset Management)

(๑.๒) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

(๑.๓) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

(๑.๔) การจัดการผู้ให้บริการภายนอก (Third Party Management)

(๒) ดำเนินการตามมาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) โดยครอบคลุมในเรื่องดังต่อไปนี้

(๒.๑) การควบคุมการเข้าถึง (Access Control)

(๒.๒) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

(๒.๓) การเชื่อมต่อระยะไกล (Remote Connection)

(๒.๔) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

(๒.๕) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ (Information and Cybersecurity Awareness)

(๒.๖) การแบ่งปันข้อมูล (Information Sharing)

(๓) ดำเนินการตามมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์และสารสนเทศ (Detect) โดยมีกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

(๔) ดำเนินการตามมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์และสารสนเทศ (Respond) โดยครอบคลุมในเรื่อง ดังต่อไปนี้

(๔.๑) แผนการรับมือภัยคุกคามทางไซเบอร์และสารสนเทศ (Information and Cybersecurity Incident Response Plan)

(๔.๒) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

(๔.๓) การฝึกซ้อมความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ (Information and Cybersecurity Exercise)

(๕) ดำเนินการตามมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์และสารสนเทศ (Recover) โดยต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของ กฟผ. สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

ข้อ ๕ ผู้บริหารและผู้ปฏิบัติงานต้องได้รับการส่งเสริมความรู้ความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

ข้อ ๖ ผู้บริหารและผู้ปฏิบัติงานมีหน้าที่ปฏิบัติตามมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ กฟผ.

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๒๐ มิถุนายน พ.ศ. ๒๕๖๗