

- ๔ -

๕) ผู้รับผิดชอบสารสนเทศต้องแบ่งแยกหน้าที่และขอบเขตความรับผิดชอบในการปฏิบัติงานอย่างชัดเจน เพื่อลดโอกาสความผิดพลาดในการเปลี่ยนแปลง หรือใช้งานระบบสารสนเทศหรือข้อมูลสารสนเทศผิดวัตถุประสงค์ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๖) หน่วยงานของ กฟผ. ที่มีหน้าที่ติดต่อกับหน่วยงานภายนอกที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่างๆ ต้องกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกนั้นไว้อย่างชัดเจน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๗) ทุกสายงานของ กฟผ. ต้องกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศภายใต้สถานการณ์ต่างๆ ไว้อย่างชัดเจน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๘) ในการดำเนินงานทุกโครงการหรือทุกแผนงานต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๙) ผู้ดูแลระบบสารสนเทศต้องลดความเสี่ยงในการใช้งานอุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้ที่เชื่อมกับระบบของ กฟผ. ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๐) ผู้ดูแลระบบสารสนเทศต้องควบคุมดูแลการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ของ กฟผ. ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๑) คณะกรรมการมีหน้าที่ดูแลรับผิดชอบการจัดการ การสนับสนุนและกำหนดทิศทาง การดำเนินงาน เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศที่ชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใดๆ

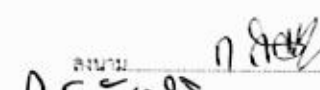
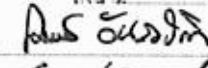
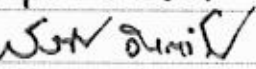
๑๒) คณะกรรมการต้องส่งเสริมให้เกิดความร่วมมือในการรักษาความมั่นคงปลอดภัยสารสนเทศในทุกภาคส่วนของ กฟผ.

๑๓) ผู้ที่นำระบบสารสนเทศใหม่มาใช้ต้องปฏิบัติตามขั้นตอนการพิจารณาทบทวน เพื่ออนุมัติการสร้าง การติดตั้ง หรือการใช้งานในแง่มุมต่างๆ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๔) การอนุญาตให้หน่วยงานภายนอกหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศของ กฟผ. ผู้รับผิดชอบสารสนเทศต้องระบุความเสี่ยง ประเมินความเสี่ยงที่อาจเกิดขึ้นและกำหนดแนวทางป้องกัน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๕) ผู้ดูแลระบบสารสนเทศต้องมีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศสำหรับการอนุญาตให้ผู้ใช้ที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของ กฟผ. ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ใน ปัจจุบัน

หน้า ๓ ...

ลงนาม		ประธานกรรมการ
ลงนาม		กรรมการ
ลงนาม		กรรมการ

- ๕ -

หมวด ๓
ความมั่นคงปลอดภัยสารสนเทศด้านบุคลากร

วัตถุประสงค์

เพื่อวางกรอบการสรรหา การควบคุมและการติดตามบุคลากรที่เข้ามาปฏิบัติงานภายใน กฟผ. รวมถึงการจ้างบุคคลหรือหน่วยงานภายนอก การบริหารจัดการบุคลากรและผู้รับจ้างระหว่างการจ้างงาน เมื่อมีการเปลี่ยนแปลงหน้าที่การปฏิบัติงาน หรือเมื่อพ้นสภาพการเป็นพนักงานหรือลูกจ้าง เพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศ

แนวนโยบาย

๑๖) หน่วยงานที่รับผิดชอบงานบุคคลและหน่วยงานที่รับผิดชอบงานจ้างหรืองานโครงการที่มีการเข้าถึงทรัพย์สินสารสนเทศของ กฟผ. ต้องตรวจสอบคุณสมบัติและประวัติของผู้สมัครงานหรือคู่สัญญาจะต้องไม่มีประวัติการกระทำผิดกฎหมายสารสนเทศ การบุกรุก แก้อี โฮ ฟ่าลาย หรือโจรกรรมข้อมูลสารสนเทศมาก่อน

๑๗) หน่วยงานด้านกฎหมายและบุคลากรของ กฟผ. ต้องระงับหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศไว้ในสัญญา หรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก โดยให้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

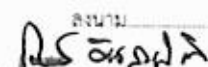
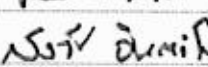
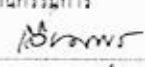
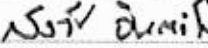

๑๘) ผู้บังคับบัญชาชั้นต้นขึ้นไปต้องกำกับดูแล และแจ้งให้พนักงานในสังกัดและบุคคลภายนอกถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๙) ผู้รับผิดชอบสารสนเทศต้องจัดอบรมและหรือสื่อสารให้ผู้ใช้ทราบถึงนโยบายหรือระเบียบ หลักเกณฑ์ และวิธีปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่ กฟผ. ประกาศใช้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศในส่วนที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตน

๒๐) การลงโทษผู้ใช้และผู้รับผิดชอบสารสนเทศที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ให้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๒๑) หัวหน้าหน่วยงานที่รับผิดชอบงานบุคคล หรือหน่วยงานที่รับผิดชอบงานจ้างหรืองานโครงการที่มีการเข้าถึงทรัพย์สินสารสนเทศของ กฟผ. ต้องแจ้งการยุติการจ้าง หรือการเปลี่ยนแปลงสภาพการจ้าง โยกย้ายหน่วยงาน การพักงาน ระเบียบการปฏิบัติหน้าที่ การปรับเปลี่ยนบุคลากร หรือการสิ้นสุดสัญญาจ้างของหน่วยงานภายนอกหรือบุคคลภายนอก หรืองานโครงการที่มีการเข้าถึงทรัพย์สินสารสนเทศของ กฟผ. ให้หน่วยงานผู้รับผิดชอบสารสนเทศทราบ เพื่อดำเนินการยกเลิกหรือเปลี่ยนแปลงสิทธิการเข้าถึงระบบสารสนเทศทันที ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๔ ...

ลงนาม		ประธานกรรมการ		
ลงนาม		กรรมการ	ลงนาม	
ลงนาม		กรรมการ	ลงนาม	

- ๗ -

คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๓๑) กรณีมีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูลสารสนเทศ เพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูล โดยไม่ได้รับอนุญาต หรือถูกนำไปใช้ในทางที่ผิด หรืออุปกรณ์ หรือข้อมูลสารสนเทศได้รับความเสียหาย ให้ผู้รับผิดชอบสารสนเทศและผู้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๕
การควบคุมการเข้าถึง

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึง การใช้งานระบบสารสนเทศของ กฟผ. และการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก รวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่สารสนเทศของ กฟผ.

แนวนโยบาย

๓๒) ให้คณะกรรมการกำหนดและทบทวนนโยบายควบคุมการเข้าถึงอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง เพื่อให้สอดคล้องกับกฎหมายหรือประกาศ และแจ้งให้ผู้ใช้รับทราบและถือปฏิบัติ

๓๓) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๓๔) ผู้ใช้ต้องมีบัญชีผู้ใช้เป็นของตนเอง และผู้รับผิดชอบสารสนเทศต้องมีเทคนิคการตรวจสอบตัวตนที่เพียงพอ เพื่อให้สามารถระบุตัวตนของผู้ใช้งานระบบสารสนเทศได้ โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๓๕) ผู้รับผิดชอบสารสนเทศต้องจัดให้มีการลงทะเบียนบัญชีใช้ระบบสารสนเทศ และยกเลิกบัญชีผู้ใช้เพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการใช้งานระบบสารสนเทศของ กฟผ. โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๓๖) เจ้าของระบบสารสนเทศต้องจำกัดจำนวน และควบคุมผู้มีสิทธิระดับสูง โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๓๗) ผู้ดูแลระบบสารสนเทศต้องกำหนดขั้นตอนการตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๓๘) หน่วยงานเจ้าของข้อมูลสารสนเทศต้องติดตามทบทวนระดับสิทธิในการเข้าถึงของผู้ใช้ตามรอบระยะเวลาที่ได้กำหนดไว้ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๓๙) หน่วยงาน ...

.....
.....
.....

- ๘ -

๓๙) หน่วยงานที่รับผิดชอบสารสนเทศต้องยกเลิกหรือเปลี่ยนแปลงสิทธิในการเข้าใช้งานระบบสารสนเทศของผู้ใช้ เมื่อได้รับแจ้งการยุติการจ้าง หรือการเปลี่ยนแปลงสภาพการจ้าง โยกย้ายหน่วยงาน การพักงาน ระเบียบการปฏิบัติหน้าที่ การปรับเปลี่ยนบุคลากร หรือการสิ้นสุดสัญญาจ้างของหน่วยงานภายนอก หรือบุคคลภายนอก หรืองานโครงการที่มีการเข้าถึงทรัพย์สินสารสนเทศของ กฟผ. เพื่อไม่ให้เกิดความเสียหายกับ กฟผ. ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๐) ผู้ใช้ต้องกำหนดรหัสผ่านในการเข้าถึงระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๑) หน่วยงานที่รับผิดชอบสารสนเทศต้องจำกัดการเข้าถึงข้อมูลสารสนเทศและฟังก์ชันต่างๆ ในแอปพลิเคชันของผู้ใช้และผู้ดูแลระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๒) ผู้ดูแลระบบสารสนเทศต้องกำหนดวิธีการ Log-on เข้าระบบปฏิบัติการคอมพิวเตอร์และระบบสารสนเทศ ให้เป็นไปอย่างปลอดภัย เพื่อป้องกันและควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๓) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ระบบสารสนเทศในความเร็วขีดขอบยุติการทำงาน (Session Time-Out) เมื่อว่างเว้นจากการใช้งาน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๔) ผู้ดูแลระบบสารสนเทศต้องจำกัดระยะเวลาการเชื่อมต่อกับระบบสารสนเทศที่มีระดับความเสี่ยงสูง เพื่อเพิ่มระดับการรักษาความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๕) ผู้รับผิดชอบสารสนเทศต้องออกแบบระบบบริหารจัดการรหัสผ่านที่สามารถทำงานแบบเชิงโต้ตอบกับผู้ใช้งาน (Interactive) และสามารถรองรับการกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๖) ผู้ดูแลระบบสารสนเทศต้องจำกัดการเข้าถึงการใช้งานโปรแกรมมอดประโยชน์ต่างๆ อย่างเข้มงวด เนื่องจากโปรแกรมดังกล่าวอาจมีความสามารถควบคุมและเปลี่ยนแปลงการทำงานของระบบสารสนเทศได้ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๗) ผู้รับผิดชอบสารสนเทศต้องจำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรม โดยไม่ได้รับอนุญาต ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๘) ผู้ดูแลระบบสารสนเทศต้องจำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๙) ผู้ดูแลระบบสารสนเทศต้องระบุและตรวจสอบอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศโดยอัตโนมัติ (Automatic equipment identification) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติ

ที่เกี่ยวข้อง ...

.....
.....
.....

- ๔ -

ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๕๐) ผู้ดูแลระบบสารสนเทศต้องควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศ ทั้งทางกายภาพและระยะไกล ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๕๑) ผู้ดูแลระบบสารสนเทศต้องควบคุมเส้นทางการไหลของข้อมูลสารสนเทศในระบบเครือข่าย คอมพิวเตอร์ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๕๒) คณะกรรมการต้องพิจารณากำหนดระบบสารสนเทศที่มีความสำคัญสูง ให้มีสภาพแวดล้อม ที่แยกออกมาต่างหาก สำหรับกรณีที่มีความจำเป็นต้องใช้ระบบสารสนเทศร่วมกันระหว่างระบบงานให้มีการประเมินความเสี่ยงสำหรับการใช้งานนั้นๆ โดยให้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๕๓) ผู้รับผิดชอบสารสนเทศต้องกำหนดวิธีการตรวจสอบตัวตนของผู้ใช้ที่เหมาะสมเพื่อควบคุม การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทาง ปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๖

การควบคุมการเข้าถึงรหัสลับข้อมูล

วัตถุประสงค์

เพื่อให้การเข้าถึงรหัสลับข้อมูลและการบริหารจัดการกุญแจเข้ารหัสลับ ทำให้ระบบสารสนเทศคงไว้ซึ่งการรักษาความลับของข้อมูลและป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

แนวนโยบาย

๕๔) คณะกรรมการต้องกำหนดมาตรฐานการเข้ารหัสลับข้อมูล ประเมินความเสี่ยงเพื่อระบุระดับ ความสำคัญ และระดับความลับที่เหมาะสมสำหรับข้อมูลที่สำคัญต้องป้องกัน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๕๕) การบริหารจัดการกุญแจในการเข้ารหัส (Key Management) ให้ผู้รับผิดชอบสารสนเทศ จัดทำแนวทางการบริหารจัดการกุญแจ (Key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับ ของ กฟผ. ที่จำเป็นต้องมีกุญแจ (Key) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับ ความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน



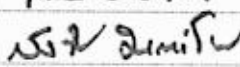
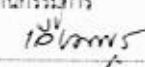

หมวด ๗

ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศ การควบคุมการใช้งานและบำรุงรักษาด้านกายภาพ ของทรัพย์สินสารสนเทศ และอุปกรณ์สารสนเทศ ซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบ สารสนเทศของ กฟผ. ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

แนวนโยบาย ...

ลงนาม  ประธานกรรมการ
 ลงนาม  กรรมการ
 ลงนาม  กรรมการ
 ลงนาม  กรรมการ
 ลงนาม  กรรมการ

แนวนโยบาย

๕๖) ผู้บังคับบัญชาชั้นต้นขึ้นไปรับผิดชอบพื้นที่ต้องป้องกันขอบเขตพื้นที่ที่ตั้งของหน่วยงาน (Security perimeter) ที่มีการติดตั้ง จัดเก็บ หรือใช้งานระบบสารสนเทศและข้อมูลสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๕๗) ผู้บังคับบัญชาชั้นต้นขึ้นไปที่สุดแลพื้นที่ที่ควบคุมต้องกำหนดให้มีบุคลากรกำกับดูแลการควบคุม การเข้าออกพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure area) โดยให้เฉพาะผู้มีสิทธิที่สามารถเข้าออก ได้ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๕๘) ผู้บังคับบัญชาชั้นต้นขึ้นไปรับผิดชอบพื้นที่ต้องออกแบบและติดตั้งการป้องกันความมั่นคง ปลอดภัยด้านกายภาพ เพื่อป้องกันและควบคุมการเข้าถึงสำนักงาน ห้องทำงาน พื้นที่ซึ่งมีข้อมูลสารสนเทศ ที่สำคัญ ห้องคอมพิวเตอร์ที่สำคัญ และพื้นที่ปฏิบัติงานของผู้รับผิดชอบสารสนเทศ หรืออุปกรณ์สารสนเทศต่างๆ

๕๙) คณะกรรมการต้องกำหนดแนวทางในการออกแบบและติดตั้งด้านกายภาพ เพื่อให้สามารถ ป้องกันภัยจากภายนอกในระดับอันตรายทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๖๐) การทำงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) ให้ผู้รับผิดชอบสารสนเทศและผู้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับ ความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๖๑) ผู้บังคับบัญชาชั้นต้นขึ้นไปต้องควบคุมการเข้าถึงพื้นที่ที่ไม่ได้รับอนุญาต และกำหนดพื้นที่ การรับส่งพัสดุ พื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าห้องคอมพิวเตอร์และควบคุมผู้ ที่มาติดต่อไม่ให้เข้าถึงพื้นที่อื่นๆ ที่ไม่ได้รับอนุญาตหรือเข้าถึงระบบสารสนเทศได้

๖๒) ผู้รับผิดชอบสารสนเทศต้องกำหนดให้มีการจัดวางและป้องกันอุปกรณ์สารสนเทศให้เหมาะสม เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต โดยพิจารณาถึงความสำคัญของอุปกรณ์ เพื่อลดความเสี่ยงจาก ภัยธรรมชาติ หรืออันตรายต่างๆ จากภัยคุกคามที่มนุษย์ก่อขึ้น ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือ แนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๖๓) ผู้รับผิดชอบสารสนเทศต้องกำหนดให้มีการป้องกันการหยุดชะงักของอุปกรณ์สารสนเทศ ที่อาจเกิดจากไฟฟ้าขัดข้อง (Power failure) หรือจากข้อผิดพลาดของระบบและอุปกรณ์ที่สนับสนุนการทำงานของ ระบบสารสนเทศ (Supporting utilities) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับ ความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๖๔) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีการป้องกันความเสียหายและสัญญาณรบกวนของ สายไฟฟ้า สายสื่อสาร รวมทั้งให้มีการป้องกันการดักจับสัญญาณ (Interception) ในช่องทางสื่อสาร

๖๕) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีการดูแลบำรุงรักษาอุปกรณ์สารสนเทศอย่างถูกวิธี เพื่อให้คงไว้ซึ่งสภาพความพร้อมใช้งานอยู่เสมอ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติ ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๖๖) การนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของ กพท. ให้ผู้รับผิดชอบสารสนเทศและผู้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติ ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๖๗) คณะกรรมการ ...

.....
.....
.....

๖๗) คณะกรรมการต้องกำหนดมาตรการรักษาความปลอดภัยอุปกรณ์สารสนเทศของ กฟผ. และอุปกรณ์ส่วนตัวที่นำมาใช้ร่วมกับระบบสารสนเทศของ กฟผ. โดยให้คำนึงถึงความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานนอกสถานที่ปฏิบัติงานของ กฟผ.

๖๘) ก่อนการยกเลิกการใช้งานหรือการนำอุปกรณ์สารสนเทศและสื่อบันทึกข้อมูลที่ใช้ในการจัดเก็บข้อมูลสารสนเทศกลับมาใช้ใหม่ ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องมีการตรวจสอบว่าได้มีการลบย้าย หรือทำลาย ข้อมูลหรือซอฟต์แวร์ที่ติดตั้งไว้ด้วยวิธีการที่ไม่สามารถกู้คืนได้อีก โดยให้ถือปฏิบัติ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๖๙) ผู้ใช้ต้องดูแลป้องกันเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และ อุปกรณ์อื่นใด ที่อยู่ภายใต้ความดูแลรับผิดชอบของตนเองในระหว่างที่ไม่มีการใช้งาน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ ในปัจจุบัน

๗๐) คณะกรรมการต้องกำหนดนโยบายปราศจากข้อมูลสารสนเทศที่สำคัญบนโต๊ะทำงานและ หน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) เพื่อป้องกันการเปิดเผยข้อมูลสารสนเทศ ที่สำคัญจากบุคคลอื่น

หมวด ๘
ความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน

วัตถุประสงค์

เพื่อควบคุมให้การปฏิบัติงาน มีขั้นตอนที่ชัดเจน พร้อมใช้งาน และมีความมั่นคงปลอดภัยสารสนเทศ

แนวนโยบาย

๗๑) ผู้ดูแลระบบสารสนเทศต้องจัดทำ ปรับปรุง และดูแล เอกสารขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ ให้มีความถูกต้องเหมาะสม และให้อยู่ในสภาพพร้อมใช้งาน เพื่อใช้ในการปฏิบัติงาน

๗๒) กรณีที่มีการเปลี่ยนแปลงของระบบสารสนเทศให้ผู้รับผิดชอบสารสนเทศถือปฏิบัติ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๗๓) ผู้รับผิดชอบสารสนเทศต้องติดตามและจัดทำแผนด้านทรัพยากรสารสนเทศเพื่อรองรับ การปฏิบัติงานในอนาคตของ กฟผ. อย่างเหมาะสม ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติ ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๗๔) ผู้รับผิดชอบสารสนเทศต้องจัดให้การแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และ ใช้งานจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับ อนุญาต ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ ของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๗๕) ผู้รับผิดชอบสารสนเทศต้องควบคุม ตรวจสอบ ป้องกัน และกู้คืนระบบสารสนเทศ จากโปรแกรมไม่พึงประสงค์ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคง ปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๗๖) ผู้รับผิดชอบสารสนเทศ ...

.....
.....
.....

- ๑๒ -

๓๖) ผู้รับผิดชอบสารสนเทศต้องตั้งค่าการทำงาน (Configuration) ห้ามไม่ให้ Mobile code สามารถทำงานในระบบสารสนเทศได้ เว้นแต่ Mobile code ที่ได้รับอนุญาตจาก กฟผ.

๓๗) ผู้รับผิดชอบสารสนเทศต้องสำรองข้อมูลสารสนเทศ และทดสอบการนำข้อมูลสำรองกลับมาใช้งาน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๓๘) ผู้รับผิดชอบสารสนเทศต้องจัดให้มีการบันทึกกิจกรรมของผู้ใช้งานระบบสารสนเทศ และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่างๆ (Audit log) เพื่อประโยชน์ในการสืบสวน สอบสวน ในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๓๙) ผู้รับผิดชอบสารสนเทศต้องมีขั้นตอนการเฝ้าติดตาม และสังเกตการใช้งานระบบสารสนเทศ พร้อมทั้งให้มีการประเมินผลการติดตามสังเกตการใช้งานระบบสารสนเทศอย่างสม่ำเสมอ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๐) ผู้รับผิดชอบสารสนเทศต้องจัดเก็บและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับข้อผิดพลาด (Fault Log) ของระบบสารสนเทศอย่างสม่ำเสมอ และจัดการแก้ไขข้อผิดพลาดที่ตรวจพบอย่างเหมาะสม ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๑) ผู้รับผิดชอบสารสนเทศต้องป้องกันการแก้ไขข้อมูลการบันทึกกิจกรรมของผู้ใช้งานระบบสารสนเทศ และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่างๆ (Audit log) รวมถึงข้อมูลที่เกี่ยวข้องกับข้อผิดพลาด (Fault Log) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๒) ผู้รับผิดชอบสารสนเทศต้องบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบสารสนเทศ (System administrator) และผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบ (System operator) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๓) ผู้ดูแลระบบสารสนเทศต้องควบคุมให้อุปกรณ์สารสนเทศ ระบบสารสนเทศของ กฟผ. ได้รับการตั้งเวลาให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง ครบถ้วนเวลาอ้างอิงสากล และต้องตรวจสอบเวลาของอุปกรณ์สารสนเทศ ระบบสารสนเทศของ กฟผ. รวมถึงปรับปรุงให้เป็นปัจจุบันเสมอ เพื่อป้องกันไม่ให้เกิดการบันทึกเวลาไม่ถูกต้อง

๔๔) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๕) ผู้รับผิดชอบสารสนเทศต้องบริหารจัดการช่องโหว่ทางเทคนิค ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๖) ผู้ดูแลระบบสารสนเทศต้องกำหนดสิทธิ์ให้ผู้ใช้ติดตั้งซอฟต์แวร์ได้เท่าที่จำเป็น ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๔๗) ผู้ตรวจสอบภายใน ...

ลงนาม		ประธานกรรมการ
ลงนาม		กรรมการ
ลงนาม		กรรมการ

- ๑๓ -

๘๗) ผู้ตรวจสอบภายในของ กฟผ. ต้องทำแผนและข้อกำหนดการตรวจสอบ รวมถึงกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ โดยได้รับความเห็นชอบจากผู้รับผิดชอบสารสนเทศ เพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของกระบวนการทางธุรกิจ

๘๘) คณะกรรมการต้องกำหนดประเภทข้อมูลตามลำดับชั้นความลับเพื่อให้ผู้รับผิดชอบสารสนเทศ และผู้ใช้ถือปฏิบัติตาม เพื่อเป็นการป้องกันไม่ให้เกิดการเข้าถึงข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) โดยไม่ได้รับอนุญาต

๘๙) คณะกรรมการต้องกำหนดนโยบายและขั้นตอนการปฏิบัติ เพื่อป้องกันข้อมูลสารสนเทศ ที่มีการสื่อสารหรือแลกเปลี่ยน หรือใช้ข้อมูลร่วมกัน ผ่านระบบสารสนเทศที่มีการเชื่อมต่อระหว่างระบบสารสนเทศต่างๆ

หมวด ๙
ความมั่นคงปลอดภัยด้านเครือข่าย

วัตถุประสงค์

เพื่อควบคุมการบริหารจัดการเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอก กฟผ. รวมถึงการควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศกับหน่วยงานภายนอกให้มีความมั่นคงปลอดภัย

แนวนโยบาย

๙๐) ผู้ดูแลระบบสารสนเทศต้องบริหารจัดการ การควบคุมเครือข่ายคอมพิวเตอร์ เครือข่ายสื่อสาร เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอปพลิเคชันที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่าย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๙๑) ผู้ดูแลระบบสารสนเทศต้องควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายทั้งหมดลงในข้อตกลง หรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายใน หรือภายนอก

๙๒) ผู้ดูแลระบบสารสนเทศต้องแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยพิจารณาตามการใช้งานในการเข้าถึงระบบเครือข่าย ผลกระทบทางด้านความมั่นคงปลอดภัยสารสนเทศ และระดับความสำคัญของข้อมูลที่อยู่บนเครือข่าย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๙๓) ผู้รับผิดชอบสารสนเทศต้องควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๙๔) ผู้รับผิดชอบสารสนเทศต้องควบคุม และให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศ หรือซอฟต์แวร์ ทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายใน กฟผ. และระหว่าง กฟผ. กับหน่วยงานภายนอก ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๙๕) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูล

อิเล็กทรอนิกส์ ...

ชื่อตำแหน่ง ประธานกรรมการ
 ชื่อตำแหน่ง กรรมการ
 ชื่อตำแหน่ง กรรมการ
 ชื่อตำแหน่ง กรรมการ
 ชื่อตำแหน่ง กรรมการ

- ๑๔ -

อิเล็กทรอนิกส์ (Electronic messaging) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๙๖) คณะกรรมการต้องกำหนด และทบทวน ข้อตกลงการรักษาข้อมูลที่เป็นความลับ (Confidentiality agreement หรือ Non-disclosure agreement) ให้กับสอดคล้องกับสถานการณ์และความต้องการของ กฟผ. ในการปกป้องข้อมูลสารสนเทศอย่างน้อยปีละ ๑ ครั้ง เพื่อใช้ประกอบสัญญาตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๑๐

ความมั่นคงปลอดภัยในการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์

เพื่อควบคุม กำกับ ติดตาม และประเมินผล ในการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศให้ทำงานได้อย่างถูกต้อง และมีความมั่นคงปลอดภัยที่ครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ

แนวนโยบาย

๙๗) หน่วยงานที่มีการจัดการหรือจัดให้มีการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ต้องระบุความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบงานที่พัฒนาขึ้นมาใช้งาน นับตั้งแต่เริ่มต้นออกแบบระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๙๘) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยไม่ได้รับอนุญาต ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๙๙) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องป้องกันมิให้มีการแก้ไขเปลี่ยนแปลงข้อมูลสารสนเทศ โดยไม่ได้รับอนุญาตและรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ ที่มีการเผยแพร่ต่อสาธารณชน ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๐๐) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยไม่ได้รับอนุญาต ให้หน่วยงานที่เกี่ยวข้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนที่มีการธุรกรรมทางออนไลน์ (Online transaction) ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๐๑) ผู้พัฒนาระบบสารสนเทศต้องพัฒนาซอฟต์แวร์และระบบสารสนเทศอย่างมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๐๒) ผู้พัฒนาระบบสารสนเทศ ...

.....	ประธานกรรมการ
.....	กรรมการ
.....	กรรมการ

๑๐๖) ผู้พัฒนาระบบสารสนเทศต้องมีขั้นตอนการควบคุมการเปลี่ยนแปลงระบบสารสนเทศ เป็นลายลักษณ์อักษร เพื่อควบคุมให้ระบบเป็นไปตามข้อกำหนดที่กำหนดไว้และมีความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๑๐๗) กรณีมีการเปลี่ยนแปลงต่อระบบปฏิบัติการคอมพิวเตอร์ของระบบสารสนเทศ ให้ผู้พัฒนาระบบสารสนเทศทดสอบและทบทวนระบบสารสนเทศนั้น เพื่อให้มั่นใจได้ว่าไม่มีผลกระทบต่อการทำงานของระบบและด้านความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๑๐๘) ผู้รับผิดชอบสารสนเทศต้องจำกัดการเปลี่ยนแปลงใดๆ ต่อซอฟต์แวร์สำเร็จรูปที่ใช้งาน (Software package) โดยให้เปลี่ยนแปลงเฉพาะเท่าที่จำเป็นและควบคุมทุกๆ การเปลี่ยนแปลงอย่างเข้มงวด เพื่อป้องกันการละเมิดลิขสิทธิ์ เพื่อความมั่นคงปลอดภัยของซอฟต์แวร์สำเร็จรูป เพื่อป้องกันผลกระทบที่ กพท. อาจต้องรับผิดชอบต่อการบำรุงรักษาซอฟต์แวร์นั้นด้วยตนเองต่อไปในอนาคต โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๑๐๙) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องพัฒนาและติดตั้งใช้งานระบบสารสนเทศโดยคำนึงถึงหลักการความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๑๐๖) ผู้พัฒนาระบบสารสนเทศต้องกำหนดมาตรการป้องกันสภาพแวดล้อมการพัฒนาแบบอย่างมั่นคงปลอดภัยให้ครอบคลุมทั้งวงจรการพัฒนาแบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๑๐๗) เจ้าของระบบสารสนเทศต้องดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์ ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

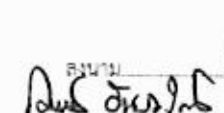
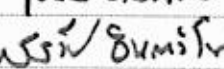
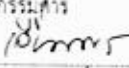

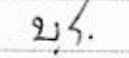
๑๐๘) ผู้พัฒนาระบบสารสนเทศต้องทดสอบด้านความมั่นคงปลอดภัยของระบบที่พัฒนาใหม่ หรือระบบงานเดิมที่ปรับปรุง เพื่อให้มั่นใจว่าระบบสารสนเทศสามารถทำงานได้อย่างมั่นคงปลอดภัยตามความต้องการที่กำหนดไว้ โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๑๐๙) หน่วยงานที่เกี่ยวข้องต้องกำหนดให้มีเกณฑ์ในการตรวจรับระบบใหม่ หรือที่ปรับปรุงเพิ่มเติม ทั้งที่มาจากการพัฒนาภายในองค์กร หรือที่มีการจัดหาจากจ้างพัฒนา และต้องทดสอบระบบก่อนที่จะนำระบบดังกล่าวมาใช้งานจริง โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๑๑๐) การนำข้อมูลมาใช้ทดสอบในระบบสารสนเทศ ให้ผู้พัฒนาระบบสารสนเทศเลือกข้อมูลมาใช้งานอย่างระมัดระวัง โดยให้มีการป้องกัน ควบคุม เพื่อไม่ให้ข้อมูลสำคัญรั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

๑๑๑) ผู้พัฒนาระบบสารสนเทศต้องตรวจสอบ (Validate) ข้อมูลใดๆ ก่อนที่จะรับเข้าสู่แอปพลิเคชันเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม โดยถือปฏิบัติตามระเบียบ

คำสั่ง ...

ลงนาม		ประธานกรรมการ	
ลงนาม		กรรมการ	ลงนาม  กรรมการ
ลงนาม		กรรมการ	ลงนาม  กรรมการ

- ๑๖ -

คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๑๒) ผู้รับผิดชอบสารสนเทศต้องตรวจสอบ (Validate) การทำงานของแอปพลิเคชันเพื่อตรวจหาข้อผิดพลาดของข้อมูลที่เกิดจากการทำงานหรือการประมวลผลที่ผิดพลาด โดยถือปฏิบัติตามระเบียบคำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๑๓) ผู้พัฒนาระบบสารสนเทศต้องรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอปพลิเคชัน เพื่อป้องกันและสร้างความมั่นใจว่าข้อมูลที่ได้รับจากการรับส่งข้อมูลเป็นข้อมูลที่ถูกต้องแท้จริง มาจากผู้ส่งที่ถูกต้อง และไม่ถูกแก้ไขระหว่างทางหรือถูกแก้ไขโดยผู้ไม่มีสิทธิ โดยถือปฏิบัติตามระเบียบคำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๑๔) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องร่วมกันดำเนินการให้มีการตรวจสอบ (Validate) ข้อมูลใดๆ อันเป็นผลจากการประมวลผลของแอปพลิเคชัน เพื่อให้มั่นใจได้ว่าข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม โดยถือปฏิบัติตามระเบียบคำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๑๕) ผู้รับผิดชอบสารสนเทศต้องป้องกันการรั่วไหลของข้อมูลสารสนเทศ โดยถือปฏิบัติตามระเบียบคำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๑๑

การจัดการความสัมพันธ์กับผู้ให้บริการภายนอก

วัตถุประสงค์

เพื่อป้องกัน ควบคุม ติดตาม และตรวจสอบ การปฏิบัติงานของหน่วยงานผู้ให้บริการภายนอก ให้มีประสิทธิภาพและมีความมั่นคงปลอดภัยสารสนเทศ

แนวนโยบาย

๑๑๖) ผู้รับผิดชอบสารสนเทศกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศในด้านต่างๆ เพื่อป้องกัน ควบคุม หรือบรรเทาความเสี่ยงจากผู้ให้บริการภายนอก ตามระเบียบคำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๑๗) สำหรับข้อตกลงเพื่ออนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนา ระบบสารสนเทศ ผู้รับผิดชอบสารสนเทศต้องระบุรายละเอียดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศตามระเบียบคำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๑๘) ผู้รับผิดชอบสารสนเทศต้องควบคุมให้มีการกำหนดข้อตกลง และความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอก โดยให้ครอบคลุมถึงผู้ให้บริการภายนอกที่รับจ้างจากผู้ให้บริการภายนอกหลักเป็นผู้จัดหา

๑๑๙) ผู้รับผิดชอบสารสนเทศ ...

.....
.....
.....

- ๑๗ -

๑๑๘) ผู้รับผิดชอบสารสนเทศต้องติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของผู้ให้บริการภายนอกที่ให้บริการแก่หน่วยงานตามที่อ้างอิงอย่างสม่ำเสมอ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๒๐) กรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน หน่วยงานที่เป็นคู่สัญญากับผู้ให้บริการภายนอกต้องประสานงานกับผู้ให้บริการภายนอกและให้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว โดยต้องรายงานให้ผู้บริหาร และผู้ที่เกี่ยวข้องรับทราบ รวมถึงให้กำหนดกระบวนการบริหารจัดการความเสี่ยงดังกล่าวให้สอดคล้องเหมาะสมตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๒๑) ผู้รับผิดชอบสารสนเทศต้องกำกับให้ผู้ให้บริการภายนอกปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการ และระดับการให้บริการ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๑๖

การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

วัตถุประสงค์

เพื่อบริหารจัดการเหตุการณ์ไม่พึงประสงค์หรือไม่อาจคาดคิดด้านความมั่นคงปลอดภัยสารสนเทศ ให้ได้รับความเสียหายน้อยที่สุด จัดเก็บปัญหาที่เกิดขึ้น และเรียนรู้ข้อผิดพลาดมาปรับปรุงแก้ไขเพื่อป้องกันไม่ให้เกิดปัญหาซ้ำอีก

แนวนโยบาย

๑๒๒) คณะกรรมการต้องกำหนดขอบเขตความรับผิดชอบของการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน


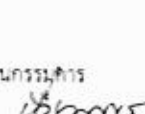
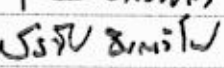
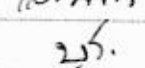


๑๒๓) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ผ่านช่องทางที่เหมาะสมโดยเร็วที่สุด โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๒๔) ผู้ใช้ต้องบันทึกและรายงานจุดอ่อนใดๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๒๕) ผู้รับผิดชอบสารสนเทศต้องมีการประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด โดยให้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๒๖) ผู้รับผิดชอบสารสนเทศต้องมีมาตรการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๒๗) คณะกรรมการ ...

ลงนาม		ประธานกรรมการ	
ลงนาม		กรรมการ	
ลงนาม		กรรมการ	

- ๑๘ -

๑๒๗) คณะกรรมการต้องกำหนดวิธีการแยกประเภท การรวบรวมปริมาณ วิเคราะห์มูลค่า ความเสียหายของเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น เพื่อใช้เป็นเกณฑ์วัดและการติดตาม เพื่อใช้ในการเรียนรู้ในการดำเนินงานและลดโอกาสเกิดในอนาคต ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือ แนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๒๘) ผู้รับผิดชอบสารสนเทศต้องรวบรวม จัดเก็บ และนำเสนอหลักฐาน หลังจากเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๑๓

การบริหารจัดการด้านการบริการ

หรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้เกิดความต่อเนื่อง

วัตถุประสงค์

เพื่อระบุเหตุการณ์ที่อาจทำให้การให้บริการสารสนเทศหยุดชะงัก การบริหารจัดการในภาวะฉุกเฉินที่มีการดำเนินงานถึงความมั่นคงปลอดภัยสารสนเทศ ให้บริการสารสนเทศดำเนินไปได้อย่างต่อเนื่อง

แนวนโยบาย

๑๒๙) ผู้รับผิดชอบสารสนเทศต้องระบุเหตุการณ์ใดๆ ที่อาจส่งผลให้การดำเนินงานหยุดชะงัก และมีความเป็นไปได้ในการเกิดผลกระทบต่อเนื่องจากการหยุดชะงักนั้น ในแง่ของความมั่นคงปลอดภัยสารสนเทศ โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๓๐) ผู้รับผิดชอบสารสนเทศต้องจัดทำข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศที่จำเป็น โดยกำหนดให้เป็นส่วนหนึ่งของขั้นตอนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

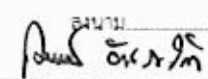
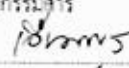
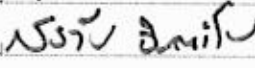

๑๓๑) ผู้รับผิดชอบสารสนเทศต้องกำหนดแผนกรณีมีเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงัก เพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศ โดยคำนึงประเด็นความมั่นคงปลอดภัยสารสนเทศ และให้สอดคล้องกับกลยุทธ์ความต่อเนื่องทางธุรกิจ ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๓๒) คณะกรรมการต้องกำหนดกรอบงาน (Framework) สำหรับการพัฒนาแผนการบริหารจัดการเพื่อการดำเนินงานทางธุรกิจมีความต่อเนื่องในภาวะฉุกเฉิน โดยคำนึงประเด็นความมั่นคงปลอดภัยสารสนเทศ และให้สอดคล้องกับกลยุทธ์ความต่อเนื่องทางธุรกิจ

๑๓๓) คณะกรรมการต้องจัดให้มีการฝึกซ้อม ทดสอบ และนำผลมาปรับปรุงแผนบริหารความต่อเนื่องให้เป็นปัจจุบันและมีประสิทธิภาพ

๑๓๔) ผู้รับผิดชอบสารสนเทศต้องประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งาน และต้องกำกับให้มีการคิดระบบสารสนเทศสำรอง หรืออุปกรณ์สำรอง หรือระบบสำหรับสนับสนุนการให้บริการที่เพียงพอ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่เหมาะสม ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๑๔ ...

ลงนาม		กรรมการ	ลงนาม		กรรมการ
ลงนาม		กรรมการ	ลงนาม		กรรมการ

- ๑๙ -

หมวด ๑๔
การปฏิบัติตามกฎระเบียบ

วัตถุประสงค์

เพื่อให้ผู้ใช้ปฏิบัติตาม รวมถึงให้มีการตรวจสอบการปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เพื่อให้การดำเนินงานของ กฟผ. เป็นไปตามกฎหมาย ระเบียบ ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยต่างๆ

แนวนโยบาย

๑๓๕) คณะกรรมการต้องรวบรวมกฎระเบียบ หลักเกณฑ์ และข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่มีความสอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่างๆ ของหน่วยงาน และจัดทำเป็นเอกสารเพื่อใช้เป็นข้อกำหนดในการปฏิบัติงานอย่างเป็นลายลักษณ์อักษร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๑๓๖) การใช้งานข้อมูลนี้อาจถือเป็นทรัพย์สินทางปัญญาหรือการใช้งานซอฟต์แวร์ที่มีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่างๆ ให้ผู้ใช้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๓๗) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องป้องกันมิให้ข้อมูลสารสนเทศที่สำคัญเกิดความเสียหาย สูญหาย หรือถูกปลอมแปลง โดยให้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๓๘) คณะกรรมการต้องจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมาย และข้อกำหนดตามสัญญาต่างๆ ของหน่วยงาน โดยให้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๓๙) ผู้รับผิดชอบสารสนเทศต้องใช้เทคนิคการเข้ารหัสลับที่สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่างๆ ของ กฟผ. โดยให้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๔๐) คณะกรรมการต้องพิจารณาทบทวน นโยบาย แนวปฏิบัติ ข้อกำหนด มาตรการต่างๆ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมาย สารสนเทศ และด้านอื่นๆ ที่เกี่ยวข้อง โดยการพิจารณาทบทวนต้องไม่มีผู้มีส่วนได้เสียกับงานเข้าร่วมพิจารณา

๑๔๑) ผู้บังคับบัญชาชั้นต้นขึ้นไปต้องกำกับดูแล ตรวจสอบ ให้พนักงานปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๔๒) ผู้รับผิดชอบสารสนเทศต้องทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับมาตรฐานการพัฒนาทางด้านความมั่นคงปลอดภัยสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๔๓) ผู้รับผิดชอบสารสนเทศต้องป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

๑๔๔) ผู้รับผิดชอบสารสนเทศ ...

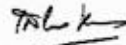
.....
.....
.....

- ๒๐ -

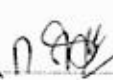
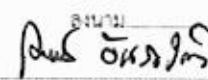
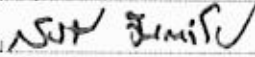
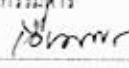

๓๔๔) ผู้รับผิดชอบสารสนเทศต้องป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อตรวจสอบเพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพค. ที่ประกาศใช้ในปัจจุบัน

ประกาศนี้ให้มีผลใช้บังคับตั้งแต่วันที่ ๒๐ ก.ค. ๒๕๖๑ เป็นต้นไป

ประกาศ ณ วันที่ ๒๐ ก.ค. ๒๕๖๑



(นายเสริมสกุล คล้ายแก้ว)
ผู้อำนวยการไฟฟ้าส่วนภูมิภาค

ลงนาม		ประธานกรรมการ		
ลงนาม		กรรมการ		
ลงนาม		กรรมการ		
		ลงนาม		กรรมการ
		ลงนาม		กรรมการ

- ๒ -

ข้อ ๖ ให้ยกเลิกความใน ๒๐) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคง ปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

“๒๐) การลงโทษผู้ใช้ที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ ของ กฟภ. ให้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคง ปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน”

ข้อ ๗ ให้ยกเลิกความใน ๒๕) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคง ปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

“๒๕) ผู้ใช้ที่ครอบครองทรัพย์สินสารสนเทศต้องส่งคืนทรัพย์สินสารสนเทศของ กฟภ. เมื่อสิ้นสุด สถานะการเป็นพนักงาน หรือสิ้นสุดสัญญา หรือสิ้นสุดข้อตกลงการปฏิบัติงาน หรือสิ้นสุดการได้รับมอบหมาย ให้ใช้ระบบสารสนเทศให้กับ กฟภ. ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับ ความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน”

ข้อ ๘ ให้ยกเลิกความใน ๒๖) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคง ปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

“๒๖) คณะกรรมการต้องจัดหมวดหมู่ข้อมูลสารสนเทศ กำหนดระดับความสำคัญ และกำหนด ชั้นความลับ เพื่อป้องกันข้อมูลสารสนเทศให้มีความปลอดภัย โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน”

ข้อ ๙ ให้ยกเลิกความใน ๒๗) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคง ปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

“๒๗) การบริหารจัดการสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ชนิดที่ถอดย้ายได้ (Removable media) ของ กฟภ. ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ ให้ผู้รับผิดชอบสารสนเทศถือปฏิบัติ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน”

ข้อ ๑๐ ให้ยกเลิกความใน ๓๔) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคง ปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

“๓๔) หน่วยงานเจ้าของข้อมูลสารสนเทศต้องติดตามทบทวนสิทธิในการเข้าถึงของผู้ใช้ตามรอบ ระยะเวลาที่ได้กำหนดไว้ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคง ปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน”

ข้อ ๑๑ ให้ยกเลิกความใน ๓๕) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคง ปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

“๓๕) ผู้ดูแลระบบสารสนเทศต้องยกเลิกหรือเปลี่ยนแปลงสิทธิในการเข้าถึงระบบสารสนเทศ ของผู้ใช้ เมื่อได้รับแจ้งการยุติการจ้าง หรือการเปลี่ยนแปลงสภาพการจ้าง โยกย้ายหน่วยงาน การพักงาน ระเบียบการปฏิบัติหน้าที่ การปรับเปลี่ยนบุคลากร หรือการสิ้นสุดสัญญาจ้าง ตามข้อ ๒๑ หรือหน่วยงาน ผู้รับผิดชอบสารสนเทศเพื่อไม่ให้เกิดความเสียหายกับ กฟภ. ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทาง ปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน”

ข้อ ๑๒ ให้ยกเลิกความใน ๔๑) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคง ปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

“๔๑) เจ้าของข้อมูลสารสนเทศต้องจำกัดการเข้าถึงข้อมูลสารสนเทศ และฟังก์ชันต่างๆ ในแอปพลิเคชันของผู้ใช้และผู้ดูแลระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติ ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน”

.....
.....
.....

- ๓ -

ข้อ ๑๓ ให้ยกเลิกความใน ๖๐) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

"๖๐) การทำงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure area) ให้ผู้รับผิดชอบสารสนเทศและผู้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน"

ข้อ ๑๔ ให้ยกเลิกความใน ๖๑) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

"๖๑) ผู้บังคับบัญชาชั้นต้นขึ้นไปรับผิดชอบพื้นที่ต้องควบคุมการเข้าถึงพื้นที่ที่ไม่ได้รับอนุญาตและกำหนดพื้นที่การรับส่งพัสดุ พื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าห้องคอมพิวเตอร์และควบคุมผู้ที่มาติดต่อไม่ให้เข้าถึงพื้นที่อื่นๆ ที่ไม่ได้รับอนุญาตหรือเข้าถึงระบบสารสนเทศได้"

ข้อ ๑๕ ให้ยกเลิกความใน ๗๖) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

"๗๖) ผู้รับผิดชอบสารสนเทศควรตั้งค่าการทำงาน (Configuration) ห้ามไม่ให้ Mobile code สามารถทำงานในระบบสารสนเทศได้ เว้นแต่ Mobile code ที่ได้รับอนุญาตจาก กฟภ."

ข้อ ๑๖ ให้ยกเลิกความใน ๘๘) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

"๘๘) หน่วยงานผู้รับผิดชอบสารสนเทศต้องป้องกันไม่ให้เกิดการรั่วไหลข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) โดยไม่ได้รับอนุญาต"

ข้อ ๑๗ ให้ยกเลิกความใน ๑๐๗) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

"๑๐๗) เจ้าของระบบสารสนเทศต้องดูแล ควบคุม ติดตามตรวจสอบการทำงานของงานในการใช้งานซอฟต์แวร์ ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน"

ข้อ ๑๘ ให้ยกเลิกความใน ๑๑๖) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน


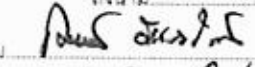
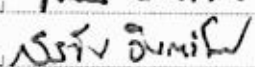
"๑๑๖) ผู้รับผิดชอบสารสนเทศต้องแจ้งให้ผู้ให้บริการภายนอกปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน"

ข้อ ๑๙ ให้ยกเลิกความใน ๑๓๐) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

"๑๓๐) ผู้รับผิดชอบสารสนเทศและหน่วยงานที่เกี่ยวข้องต้องจัดทำข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศที่จำเป็น โดยกำหนดให้เป็นส่วนหนึ่งของการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน"

ข้อ ๒๐ ให้ยกเลิกความใน ๑๓๖) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

"๑๓๖) การใช้งานข้อมูลที่เกี่ยวข้องเป็นทรัพย์สินทางปัญญาหรือการใช้งานซอฟต์แวร์ต้องมีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่างๆ โดยให้ผู้รับผิดชอบสารสนเทศปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน"

ลงนาม  ประธานกรรมการ
 ลงนาม  กรรมการ
 ลงนาม  กรรมการ

ประธานกรรมการ
 กรรมการ
 กรรมการ

- ๔ -

ข้อ ๒๑ ให้ยกเลิกความใน ๑๔๐) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

*๑๔๐) คณะกรรมการต้องพิจารณาทบทวนนโยบาย แนวทางปฏิบัติ ข้อกำหนด มาตรการต่างๆ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมาย สารสนเทศ และด้านอื่นๆ ที่เกี่ยวข้อง โดยการพิจารณาทบทวนต้องไม่มีผู้มีส่วนได้เสียกับงานเข้าร่วมพิจารณา"

ประกาศ ณ วันที่ ๑๙ สิงหาคม ๒๕๖๒



(นายสมพงษ์ ปรีเปรม)
ผู้ว่าการการไฟฟ้าส่วนภูมิภาค

ลงนาม		ประธานกรรมการ	
ลงนาม		กรรมการ	ลงนาม  กรรมการ
ลงนาม		กรรมการ	ลงนาม  กรรมการ



การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

สัญญารักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement)
และการปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

สัญญาฉบับนี้ ทำขึ้นที่ สำนักงานใหญ่ การไฟฟ้าส่วนภูมิภาค ตั้งอยู่เลขที่ 200 ถนนงามวงศ์วาน แขวง
ลาดยาว เขตจตุจักร กรุงเทพมหานคร รหัสไปรษณีย์ 10900 เมื่อวันที่.....
ระหว่าง การไฟฟ้าส่วนภูมิภาค โดย.....ซึ่งต่อไปนี้เรียกว่า
“ผู้ให้ข้อมูล” ฝ่ายหนึ่ง กับ.....
โดย.....
ซึ่งมีนิติสัมพันธ์กับ การไฟฟ้าส่วนภูมิภาค ตาม.....
.....(ระบุนรายละเอียดของสัญญา/ข้อตกลง/โครงการ/การวิจัย/)
.....
ซึ่งต่อไปนี้เรียกว่า “ผู้รับข้อมูล” อีกฝ่ายหนึ่ง

ทั้งสองสัญญาได้ตกลงกัน โดยมีข้อความดังต่อไปนี้

ข้อ 1. คำนิยาม

“ข้อมูลที่เป็นความลับ” หมายความว่า บรรดาข้อความ เอกสาร ข้อมูล ตลอดจนรายละเอียดทั้ง
ปวงที่เป็นของผู้ให้ข้อมูล รวมถึงที่อยู่ในความครอบครองหรือควบคุมดูแลของผู้ให้ข้อมูล และไม่เป็นที่รับรู้ของ
สาธารณชนโดยทั่วไป ไม่ว่าจะในรูปแบบที่จับต้องได้หรือไม่ หรือสื่อแบบใด ไม่ว่าจะถูกดัดแปลงแก้ไขโดยผู้รับข้อมูล
หรือไม่ และไม่ว่าจะเปิดเผยเมื่อใดและอย่างไร ให้ถือว่าเป็นความลับ

ข้อ 2. การรักษาข้อมูลที่เป็นความลับ

2.1 ผู้รับข้อมูลต้องรับผิดชอบรักษาข้อมูลที่เป็นความลับ และเก็บข้อมูลความลับไว้โดย
ครบถ้วน และอย่างเคร่งครัด ผู้รับข้อมูลจะต้องไม่เปิดเผย ทำสำเนา หรือทำการอื่นใดทำนองเดียวกันแก่บุคคลอื่น
ไม่ว่าทั้งหมดหรือบางส่วน เว้นแต่ได้รับอนุญาตเป็นหนังสือจากผู้ให้ข้อมูล

2.2 ผู้รับข้อมูลต้องใช้ข้อมูลที่เป็นความลับเพื่อการอันเกี่ยวกับหรือสัมพันธ์กับการดำเนินงานที่มี
อยู่ระหว่างผู้ให้ข้อมูลกับผู้รับข้อมูล โดยผู้รับข้อมูลต้องแจ้งให้ผู้ให้ข้อมูลทราบโดยทันทีที่พบการใช้หรือการเปิดเผย
ข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต หรือการละเมิดหรือฝ่าฝืนข้อกำหนดตามสัญญานี้ อีกทั้งผู้รับข้อมูลจะต้อง
ให้ความร่วมมือกับผู้ให้ข้อมูลอย่างเต็มที่ในการเรียกคืนซึ่งการครอบครองข้อมูลที่เป็นความลับ การป้องกันการใช้
ข้อมูลที่เป็นความลับโดยไม่ได้รับอนุญาต และการระงับยับยั้งการเผยแพร่ข้อมูลที่เป็นความลับออกสู่สาธารณะ

2.3 ผู้รับข้อมูลต้องใช้มาตรการที่เหมาะสมในการเก็บรักษาข้อมูลที่เป็นความลับ เพื่อป้องกันมิ
ให้ข้อมูลที่เป็นความลับถูกนำไปใช้โดยไม่ได้รับอนุญาตหรือถูกเปิดเผยแก่บุคคลอื่น โดยผู้รับข้อมูลต้องใช้มาตรการการ

ลงนาม..... ก. ก. ก. ก. ประธานกรรมการ
ลงนาม..... ธรรมการ ลงนาม..... ธรรมการ
ลงนาม..... ธรรมการ ลงนาม..... ธรรมการ

เก็บรักษาข้อมูลที่เป็นความลับในระดับเดียวกันกับที่ผู้รับข้อมูลใช้กับข้อมูลที่เป็นความลับของตนเอง ซึ่งต้องไม่น้อยกว่าการดูแลที่สมควร

2.4 ผู้รับข้อมูลต้องแจ้งให้บุคลากร พนักงาน ลูกจ้าง ที่ปรึกษาของผู้รับข้อมูล และ/หรือ บุคคลภายนอกที่เกี่ยวข้องกับข้อมูลที่เป็นความลับนั้นทราบถึงความเป็นความลับและข้อจำกัดสิทธิในการใช้และการเปิดเผยข้อมูลที่เป็นความลับ และผู้รับข้อมูลต้องดำเนินการให้บุคคลดังกล่าวต้องผูกพันด้วยสัญญาหรือข้อตกลงเป็นหนังสือในการรักษาข้อมูลที่เป็นความลับโดยมีข้อกำหนดเช่นเดียวกับหรือไม่น้อยกว่าข้อกำหนดและเงื่อนไขในสัญญาฉบับนี้ด้วย

2.5 ข้อมูลที่เป็นความลับตามข้อตกลงฉบับนี้ ไม่รวมไปถึงข้อมูลดังต่อไปนี้

- (1) ข้อมูลที่ ผู้ให้ข้อมูล เปิดเผยแก่สาธารณะ
- (2) ข้อมูลที่ผู้รับข้อมูลทราบอยู่ก่อนที่ ผู้ให้ข้อมูล จะเปิดเผยข้อมูลนั้น
- (3) ข้อมูลที่มาจากการพัฒนาโดยอิสระของผู้รับข้อมูลเอง
- (4) ข้อมูลที่ต้องเปิดเผยโดยกฎหมายหรือตามคำสั่งศาล ทั้งนี้ผู้รับข้อมูลต้องมีหนังสือแจ้งให้ ผู้ให้ข้อมูล ได้รับทราบถึงข้อกำหนดหรือคำสั่งดังกล่าวพร้อมทั้งหมายศาล และ/หรือ หมายค้นอย่างเป็นทางการยื่นต่อผู้ให้ข้อมูล ก่อนที่จะดำเนินการเปิดเผยข้อมูลดังกล่าว และในการเปิดเผยข้อมูลดังกล่าวผู้รับข้อมูลจะต้องดำเนินการตามขั้นตอนทางกฎหมายเพื่อขอให้คุ้มครองข้อมูลดังกล่าวไม่ให้ถูกเปิดเผยต่อสาธารณะด้วย
- (5) เป็นการเปิดเผยข้อมูลโดยได้รับความเห็นชอบจากผู้ให้ข้อมูล เป็นลายลักษณ์อักษร ก่อนที่ผู้รับข้อมูลจะเปิดเผยข้อมูลนั้น

ข้อ 3. ทรัพย์สินทางปัญญา

สัญญาฉบับนี้ไม่มีผลบังคับใช้เป็นการโอนสิทธิหรือการอนุญาตให้ใช้สิทธิ (ไม่ว่าโดยตรง หรือโดยอ้อม) ให้แก่ผู้รับข้อมูลที่ได้รับ ความลับซึ่ง สิทธิบัตร ลิขสิทธิ์ การออกแบบ เครื่องหมายการค้า ตราสัญลักษณ์ รูป ประติมากรรมอื่นใด ชื่อทางการค้า ความลับทางการค้า ไม่ว่าจะจดทะเบียนไว้ตามกฎหมายหรือไม่ก็ตาม หรือสิทธิอื่นๆ ของผู้ให้ข้อมูล ซึ่งอาจมีอยู่ใน ปรากฏอยู่ หรือนำมาทำซ้ำไว้ในเอกสารข้อมูลที่เป็นความลับ ทั้งนี้ ผู้รับข้อมูลหรือบุคคลอื่นใดที่เกี่ยวข้องกับผู้รับข้อมูล และเกี่ยวข้องกับข้อมูลที่เป็นความลับดังกล่าว จะไม่ยื่นขอรับสิทธิและหรือขอจดทะเบียนเกี่ยวกับทรัพย์สินทางปัญญาใดๆ ตลอดจนไม่นำไปใช้โดยไม่ได้รับการอนุญาตเป็นหนังสือจากผู้ให้ข้อมูล เกี่ยวกับรายละเอียดข้อมูลที่เป็นความลับหรือส่วนหนึ่งส่วนใดของรายละเอียดดังกล่าว

ข้อ 4. หน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ

ผู้รับข้อมูลต้องปฏิบัติตามนโยบาย แนวปฏิบัติ หลักเกณฑ์ ประกาศ ระเบียบ หรือกฎหมายเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ บรรดาซึ่งใช้บังคับอยู่ในปัจจุบัน รวมทั้งที่จะมีการประกาศใช้ ในอนาคตด้วย

ในกรณีผู้รับข้อมูลมีการดำเนินการที่เกี่ยวข้องกับระบบสารสนเทศของผู้ให้ข้อมูล นอกจากจะต้องการดำเนินการตามวรรคแรกแล้ว ผู้รับข้อมูลต้องปฏิบัติตามสปรายละเอียดนโยบายด้านความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการภายนอก และต้องดำเนินการให้ถูกต้องสอดคล้องตามนโยบายการพัฒนาระบบสารสนเทศด้วย

ลงนาม.....ประธานกรรมการ
ลงนาม.....กรรมการ
ลงนาม.....กรรมการ

ข้อ 5. การส่งคืน ลบ หรือการทำลายข้อมูลที่เป็นความลับ

เมื่อการดำเนินงานที่มีอยู่ระหว่างผู้ให้ข้อมูลกับผู้รับข้อมูลเสร็จสิ้นลง ผู้รับข้อมูลจะต้องส่งมอบข้อมูลที่เป็นความลับและสำเนาของข้อมูลที่เป็นความลับที่ผู้รับข้อมูลได้รับไว้คืนให้แก่ผู้ให้ข้อมูล ตลอดจนลบหรือทำลายข้อมูลที่เป็นความลับที่ถูกจัดเก็บไว้ในคอมพิวเตอร์ หรืออุปกรณ์อื่นใดที่ใช้จัดเก็บข้อมูล (ถ้ามี) หรือดำเนินการอื่นตามที่ได้รับการแจ้งเป็นหนังสือจากผู้ให้ข้อมูล ตลอดจนยุติการใช้ข้อมูลที่เป็นความลับที่ได้จากผู้ให้ข้อมูลทันที และผู้รับข้อมูลจะต้องรักษาความลับของข้อมูลที่ได้รับจากผู้ให้ข้อมูลตลอดไป แม้ว่าการดำเนินงานเสร็จสิ้นลงแล้วก็ตาม

ข้อ 6. การชดใช้ค่าเสียหาย

ในกรณีที่ผู้รับข้อมูล และ/หรือบุคคลที่ได้รับข้อมูลที่เป็นความลับตามสัญญาซึ่งอยู่ในความรับผิดชอบดูแลของผู้รับข้อมูล ผ่าฝืนข้อกำหนดตามข้อตกลงนี้ และก่อให้เกิดความเสียหายแก่ผู้ให้ข้อมูล ผู้รับข้อมูลจะต้องชดใช้ค่าเสียหายที่เกิดขึ้นทั้งหมดให้แก่ผู้ให้ข้อมูลภายใน ๓๐ (สามสิบ) วัน นับแต่ได้รับหนังสือแจ้งค่าเสียหาย

ข้อ 7. การบังคับใช้

7.1 ในกรณีที่ปรากฏในภายหลังว่าส่วนใดส่วนหนึ่งในสัญญาดังนี้เป็นโมฆะ ให้ถือว่าข้อกำหนดส่วนที่เป็นโมฆะไม่มีผลบังคับในสัญญานี้ และข้อกำหนดที่เหลืออยู่ในสัญญาดังนี้ ยังคงใช้บังคับและมีผลอยู่อย่างสมบูรณ์

7.2 สัญญาดังนี้อยู่ภายใต้การบังคับใช้และตีความตามกฎหมายไทย

สัญญานี้ทำขึ้นสองฉบับ มีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความโดยละเอียดตลอดแล้ว จึงได้ลงลายมือชื่อพร้อมทั้งประทับตรา (ถ้ามี) ไว้เป็นสำคัญต่อหน้าพยานและคู่สัญญาต่างยึดถือไว้ฝ่ายละหนึ่งฉบับ

ลงชื่อ ผู้ให้ข้อมูล
(.....)

ลงชื่อ ผู้รับข้อมูล
(.....)

ลงชื่อ พยาน
(.....)

ลงชื่อ พยาน
(.....)

ลงนาม ประธานกรรมการ
ลงนาม กรรมการ
ลงนาม กรรมการ
ลงนาม กรรมการ