ผู้ว่าการ
วันที่ 20 ก.ค. 61 เวลา 15.14 น.
เลขที่รับ 4005

สรก.(ทส)
เลขรับที่ 2497 วันที่ 2/7/61

การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

จาก คณะอนุกรรมการจัดทำนโยบายฯ ถึง ประธานกรรมการฯ (รผก.(ทส))

เลขที่ กมส.(มส) ๕๓๐ /๒๕๖๑ วันที่ ๒๘ มิ.ย. ๒๕๖๑

เรื่อง ขออนุมัติยกเลิกนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ พ.ศ. ๒๕๕๘ และขออนุมัติใช้นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑

เรียน ประธานกรรมการฯ (รผก.(ทส))

๑. เรื่องเดิม

ตามอนุมัติ ผวก. ลงวันที่ ๔ ตุลาคม ๒๕๖๐ เรื่อง ขออนุมัติยกเลิกระเบียบการไฟฟ้าส่วนภูมิภาคว่าด้วยการใช้งานสารสนเทศ พ.ศ. ๒๕๕๕ และขออนุมัติใช้ระเบียบการไฟฟ้าส่วนภูมิภาคว่าด้วยการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐ (เอกสารแนบ ๑) ซึ่งในระเบียบฯ ข้อ ๓.๓ กำหนดให้ ฝสท., ฝคฟ., ฝวร., ฝมป., ฝสค. และ ฝพท. ร่วมกันจัดทำแนวปฏิบัติ วิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติการจัดการและความมั่นคงปลอดภัย ด้านสารสนเทศ (ตามระเบียบการไฟฟ้าส่วนภูมิภาคว่าด้วยการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐ ภาคผนวก ก ข้อ ๑) ให้แล้วเสร็จภายใน ๑๘๐ วัน นับถัดจากวันที่ ผวก. ลงนาม

๒. ข้อเท็จจริง

๒.๑. ตามที่ ผวก. ได้มีคำสั่งแต่งตั้งคณะกรรมการ การจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ ตามคำสั่งการไฟฟ้าส่วนภูมิภาค ที่ พ.(ก) ๑๔/๒๕๖๑ ลงวันที่ ๑๗ มกราคม ๒๕๖๑ (เอกสารแนบ ๒) ข้อ ๖ ให้คณะกรรมการฯ มีอำนาจแต่งตั้งคณะอนุกรรมการ มอบหมายบุคคล และหรือหน่วยงานได้ตามความจำเป็นและเหมาะสม เพื่อปฏิบัติงานใดๆ ตามที่คณะกรรมการฯ มอบหมาย

๒.๒. ประธานกรรมการการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ ได้มีคำสั่งแต่งตั้งคณะอนุกรรมการจัดทำนโยบาย แนวปฏิบัติ วิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ โดยให้แต่ละฝ่ายจัดส่งรายชื่อผู้แทนจากกองที่เกี่ยวข้องเพื่อร่วมเป็นคณะอนุกรรมการฯ ตามคำสั่งการไฟฟ้าส่วนภูมิภาค ที่ พ.(ก) ๘๗/๒๕๖๑ ลงวันที่ ๒๖ กุมภาพันธ์ ๒๕๖๑ (เอกสารแนบ ๓) โดยมีหน้าที่ดังนี้

๒.๒.๑. จัดทำนโยบาย แนวปฏิบัติ วิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติการจัดการเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศ ตามระเบียบการไฟฟ้าส่วนภูมิภาคว่าด้วยการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐

๒.๒.๒. รายงานความคืบหน้าให้กับคณะกรรมการการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศทราบ

๒.๒.๓. สามารถเชิญหน่วยงานที่เกี่ยวข้องมาร่วมประชุมได้ตามความเหมาะสม

๒.๒.๔. นำเสนอคณะกรรมการการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศพิจารณาขออนุมัติใช้งาน

๓. ข้อพิจารณา...

๓. ข้อพิจารณา และการดำเนินการของคณะอนุกรรมการฯ

ตามข้อเท็จจริงดังกล่าวข้างต้น คณะอนุกรรมการฯ พิจารณาแล้วเห็นว่าเพื่อให้การดำเนินงานของ กฟภ. เป็นไปด้วยความเรียบร้อยและเป็นไปตามที่กฎหมายกำหนด คณะอนุกรรมการฯ จึงได้รวบรวมประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕, มาตรฐาน ISO/IEC 27001 รวมทั้งระเบียบหลักเกณฑ์ วิธีปฏิบัติที่เกี่ยวข้อง มาเป็นแนวทางในการจัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ ซึ่งมีรายละเอียดเนื้อหาที่ต้องพิจารณา ตีความ และทบทวนให้ครอบคลุม ครบถ้วน ถึงกิจกรรมและกระบวนงาน เพื่อให้สอดคล้องกับการทำงานหลักของ กฟภ. โดยมีส่วนเกี่ยวข้องกับหลายหน่วยงาน คณะอนุกรรมการฯ จึงได้เชิญหน่วยงานที่เกี่ยวข้องเข้าร่วมประชุมหารือเพื่อให้ได้ข้อมูลในการจัดทำนโยบายฯ ถูกต้องครบถ้วน โดยได้มีการร่วมประชุมหารือตามวันเวลา ดังนี้

วันที่	เดือน / ปี	เวลา
๒๖	กุมภาพันธ์ ๒๕๖๑	๐๙.๓๐ – ๑๖.๓๐ น.
๕, ๑๒, ๑๙, ๒๖	มีนาคม ๒๕๖๑	๐๙.๓๐ – ๑๖.๓๐ น.
๒, ๙, ๑๘, ๒๓, ๓๐	เมษายน ๒๕๖๑	๐๙.๓๐ – ๑๖.๓๐ น.
๒, ๗, ๙, ๑๕, ๑๗, ๒๑, ๒๓, ๒๘, ๓๑	พฤษภาคม ๒๕๖๑	๐๙.๓๐ – ๑๖.๓๐ น.
๑๑, ๑๓, ๑๕	มิถุนายน ๒๕๖๑	๐๙.๓๐ – ๑๖.๓๐ น.

จากการร่วมประชุมหารือและดำเนินการของอนุกรรมการฯ พอสรุปได้ดังนี้

๓.๑. คณะอนุกรรมการได้จัดทำนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ เรียบร้อยแล้ว (เอกสารแนบ ๔) โดยคณะอนุกรรมการฯ พิจารณาแยกเป็นหมวดๆ รวมทั้งสิ้น ๑๔ หมวด จำนวน ๑๔๔ ข้อ ซึ่งนโยบายฯ ดังกล่าวมีความสอดคล้องและเป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕ และมาตรฐาน ISO/IEC 27001

๓.๒. ในส่วนการจัดทำแนวปฏิบัติ วิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศนั้น คณะอนุกรรมการฯ ได้พิจารณาในเบื้องต้นแล้วเห็นว่าจำเป็นต้องมีการปรับปรุง แก้ไขเพิ่มเติม หรือจัดทำขึ้นใหม่ เพื่อให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ ตามตารางการจัดทำแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ (เอกสารแนบ ๕) ซึ่งในการดำเนินการดังกล่าวต้องใช้ข้อมูล รายละเอียด ลักษณะงาน กระบวนงาน และความชำนาญเฉพาะด้าน คณะอนุกรรมการฯ จึงเห็นควรดำเนินการดังนี้

๓.๒.๑. นำแนวปฏิบัติ วิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศที่ กฟภ. ประกาศใช้ในปัจจุบัน (เอกสารแนบ ๖) มาใช้ก่อน

๓.๒.๒. ให้ ฝสท., ฝคพ., ฝวร., ฝมป., ฝสค., ฝพท. จัดทำ ปรับปรุง แก้ไข แนวปฏิบัติ วิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ ให้ครอบคลุม ครบถ้วน ถึงกิจกรรมและกระบวนงาน เพื่อให้สอดคล้องกับการทำงานหลักของแต่ละฝ่าย ตามแนวทางของนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ ให้แล้วเสร็จภายใน ๑๘๐ วัน นับถัดจากวันที่ ผวก. ลงนามสั่งการ และนำเสนอคณะอนุกรรมการฯ พิจารณาให้แล้วเสร็จภายใน ๙๐ วัน เพื่อนำเสนอคณะกรรมการฯ พิจารณาต่อไป

๔. ข้อเสนอ ...

๔. ข้อเสนอ

จากข้อเท็จจริง ข้อพิจารณาและการดำเนินการของคณะอนุกรรมการฯ ดังกล่าวข้างต้น คณะอนุกรรมการจัดทำนโยบาย แนวปฏิบัติ วิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ พิจารณาแล้วเห็นควรนำเสนอคณะกรรมการการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อพิจารณานำเสนอ ผวก. ดังนี้

๔.๑. อนุมัติยกเลิกนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ พ.ศ. ๒๕๕๘ (เอกสารแนบ ๗)

๔.๒. อนุมัติใช้นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ ตามข้อ ๓.๑

๔.๓. อนุมัติให้นำแนวทางปฏิบัติความมั่นคงปลอดภัยสำหรับสารสนเทศที่ กฟภ. ประกาศใช้ ตามข้อ ๓.๒.๑ ถือปฏิบัติจนกว่าการจัดทำแนวทางปฏิบัติฯ ข้อ ๔.๔ จะแล้วเสร็จ

๔.๔. สั่งการให้ ฝคฟ., ฝวร., ฝมป., ฝสท., ฝสค., ฝพท. และ ฝวส. จัดทำ ปรับปรุง แก้ไข แนวปฏิบัติ วิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ ให้ครอบคลุมครบถ้วน ถึงกิจกรรมและกระบวนงาน เพื่อให้สอดคล้องกับการทำงานหลักของแต่ละฝ่าย ตามข้อ ๓.๒.๒

๔.๕. ลงนามในประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบขอได้โปรดนำเสนอ ผวก. เพื่อพิจารณาอนุมัติข้อ ๔.๑ ถึง ข้อ ๔.๓ พิจารณาสั่งการข้อ ๔.๔ และลงนามข้อ ๔.๕ ตามข้อเสนอต่อไป

ลงชื่อ ..... ประธานอนุกรรมการ
(นายระพีพร ภาสบุตร)
รฝ.คฟ.

ลงชื่อ ..... รองประธานอนุกรรมการ
(นายทนงศักดิ์ กิจโรณี)
รก.มส.

ลงชื่อ ...

ลงชื่อ..... อนุกรรมการ
(นายสุภกร ศรีตุลานนท์)
รก.ผร.

ลงชื่อ..... อนุกรรมการ
(นายเศกสิทธิ์ ทองทา)
ชก.พร.

ลงชื่อ..... อนุกรรมการ
(นางสาวสุวลี ดวงโชคไชย)
นรค.๙ กพก.

ลงชื่อ..... อนุกรรมการ
(นายมารุต ฆโนทัย)
วศก.๙ กอค.

ลงชื่อ..... อนุกรรมการ
(นางสาวกนกวรรณ รบมีชัย)
หผ.มส. กมส.

ลงชื่อ..... อนุกรรมการ
(นายพศนน สัตพงศ์พันธุ์)
นตก.๕ กปร.

ลงชื่อ..... อนุกรรมการ
(นายเกรียงศักดิ์ กาญวัฒนะกิจ)
ชก.ปร.

ลงชื่อ..... อนุกรรมการ
(นางจุฑามาศ เอมเปรมศิลป์)
นรค.๙ กพล.

ลงชื่อ..... อนุกรรมการ
(นายศุภวัชร สุขมาก)
นรค.๙ กบข.

ลงชื่อ..... อนุกรรมการ
(นายศึกษิต ศรีพิชญพันธ์)
หผ.อร ศสฟ.

ลงชื่อ..... อนุกรรมการ
(นายรังสิวุฒิ หมื่นยา)
ชผ.ทภ. กผร.

ลงชื่อ..... อนุกรรมการและเลขานุการ
(นายเอกพล เจริญวานิช)
ชผ.มส. กมส.

เรียน ผวก.

เพื่อโปรดพิจารณาอนุมัติตามข้อ ๔.๑ - ๔.๓ พิจารณาสั่งการตามข้อ ๔.๔ และลงนามในประกาศการไฟฟ้าส่วนภูมิภาคตามข้อ ๔.๕ ตามที่คณะอนุกรรมการจัดทำนโยบายฯ เสนอต่อไป

(นายสุวัฒน์ เชี่ยวชาญชัย)
รผก.(ทส)
ประธานกรรมการฯ
- ๒ ก.ค. ๒๕๖๑

- อนุมัติตามเสนอ
- ลงนามแล้ว

(นายเสริมสกุล คล้ายแก้ว)
ผวก.
๒๐ ก.ค. ๒๕๖๑

การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

ประกาศการไฟฟ้าส่วนภูมิภาค
เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ
พ.ศ. ๒๕๖๑

.....

การไฟฟ้าส่วนภูมิภาค เป็นหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. ๒๕๕๙ รวมทั้งกฎหมายที่เกี่ยวข้อง โดยให้ครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

อาศัยอำนาจตามความแห่งพระราชบัญญัติการไฟฟ้าส่วนภูมิภาค พ.ศ. ๒๕๐๓ ที่ใช้บังคับอยู่ในปัจจุบัน การไฟฟ้าส่วนภูมิภาค จึงวางนโยบายความมั่นคงปลอดภัยสารสนเทศ ไว้ดังต่อไปนี้

คำนิยาม

"กฟภ." หมายความว่า การไฟฟ้าส่วนภูมิภาค

"คณะกรรมการ" หมายความว่า คณะกรรมการ การจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ

"ปี" หมายความว่า ปีปฏิทิน

"ทรัพย์สินสารสนเทศ" หมายความว่า

(๑) ระบบเครือข่าย ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

(๒) เครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

(๓) ซอฟต์แวร์

(๔) ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์

(๕) ลิขสิทธิ์ (Copyright) สิทธิการใช้งาน (License) ทรัพย์สินทางปัญญา (Intellectual property)

"ระบบสารสนเทศ" ...

"ระบบสารสนเทศ" หมายความว่า ระบบพื้นฐานของการทำงานต่างๆ ในรูปแบบของการจัดเก็บ การจัดการ เผยแพร่ องค์ประกอบของระบบสารสนเทศ คือระบบคอมพิวเตอร์, ระบบเครือข่าย, บุคคล, กระบวนการ, ข้อมูล, เทคโนโลยี และสถานที่

"สารสนเทศ" หมายความว่า สิ่งที่ใช้สื่อหรือส่งความหมายใดๆ ซึ่งสร้างประโยชน์ต่างๆ ได้

"ระบบเครือข่าย" หมายความว่า กลุ่มของคอมพิวเตอร์หรืออุปกรณ์สื่อสารที่เชื่อมต่อกันเพื่อให้สามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และใช้อุปกรณ์ต่างๆ ร่วมกันได้

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ซอฟต์แวร์ (software)" หมายความว่า ชุดคำสั่งหรือโปรแกรมที่ใช้สั่งงานให้คอมพิวเตอร์ทำงานตามความต้องการ

"ข้อมูล" หมายความว่า เรื่องราว หรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใดๆ

"ข้อมูลสารสนเทศ" หมายความว่า ข้อมูลที่มีความหมาย ความสัมพันธ์จากการประมวลผลที่ผู้ใช้เข้าใจ และสามารถนำไปใช้ประโยชน์ในการบริหารจัดการ ตัดสินใจ และอื่นๆ ได้

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อมูลสารสนเทศ ข้อความ ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"ข้อมูลอิเล็กทรอนิกส์" หมายความว่า ข้อความที่ได้สร้างขึ้น ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ หรือโทรสาร เป็นต้น และให้หมายความรวมถึงข้อมูลสารสนเทศด้วย

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่า การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้ของระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

"ผู้ใช้" หมายความว่า พนักงาน ลูกจ้าง ผู้ที่ได้รับสิทธิการใช้ระบบสารสนเทศจากผู้รับผิดชอบสารสนเทศ หรือได้รับมอบหมายให้ใช้ระบบสารสนเทศจากผู้บังคับบัญชา รวมถึงผู้ซึ่งได้รับความยินยอมให้ทำงานหรือทำผลประโยชน์ให้แก่หรือในสถานประกอบกิจการของ กฟภ. ไม่ว่าจะเรียกชื่ออย่างไรก็ตาม

"เจ้าของระบบสารสนเทศ" หมายความว่า หน่วยงานที่มีหน้าที่ในการจัดให้มี การพัฒนา การเชื่อมโยง การปรับปรุงแก้ไข การปฏิบัติงาน การรักษาความมั่นคงปลอดภัย และการดูแลรักษาระบบสารสนเทศร่วมกับเจ้าของข้อมูลสารสนเทศ และหรือผู้ดูแลระบบสารสนเทศและหรือผู้พัฒนาระบบสารสนเทศ

"เจ้าของข้อมูลสารสนเทศ" หมายความว่า หน่วยงานที่สามารถอนุญาต หรือปฏิเสธการเข้าถึงข้อมูล และเป็นผู้รับผิดชอบต่อความถูกต้อง ทันสมัย ความสมบูรณ์ และการทำลาย รวมถึงกำหนดระดับชั้นความลับ สิทธิ์การใช้งาน และความปลอดภัยของข้อมูลสารสนเทศ

"ผู้ดูแลระบบสารสนเทศ" หมายความว่า หน่วยงานและหรือเจ้าหน้าที่ที่บริหารจัดการทรัพย์สินสารสนเทศ ให้เป็นไปตามข้อกำหนดหรือมาตรการ หรือความมั่นคงปลอดภัยด้านสารสนเทศ ให้แก่เจ้าของข้อมูลสารสนเทศ เจ้าของระบบสารสนเทศ และหรือผู้พัฒนาระบบสารสนเทศ

"ผู้พัฒนาระบบสารสนเทศ" ...

"ผู้พัฒนาระบบสารสนเทศ" หมายความว่า หน่วยงานที่ทำหน้าที่ในการจัดให้ได้มาซึ่งการพัฒนาระบบสารสนเทศให้กับหน่วยงาน

"ผู้รับผิดชอบสารสนเทศ" หมายความว่า เจ้าของระบบสารสนเทศ เจ้าของข้อมูลสารสนเทศ ผู้ดูแลระบบสารสนเทศ ผู้พัฒนาระบบสารสนเทศ

"ระดับชั้นความลับ" หมายความว่า การกำหนดการเปิดเผยข้อมูลสารสนเทศต่อผู้อื่นให้เหมาะสมกับสถานะการ ใช้งาน เช่น ลับที่สุด ลับมาก ลับ ปกปิด เปิดเผยสู่ภายนอกได้ เป็นต้น

"โปรแกรมอรรถประโยชน์" หมายความว่า โปรแกรมที่ผู้ดูแลระบบสารสนเทศใช้ในการบริหารจัดการระบบสารสนเทศ รวมถึงเครื่องมือที่ใช้ในการทดสอบด้านความมั่นคงปลอดภัยระบบสารสนเทศ เช่น ซอฟต์แวร์ที่ใช้ในการสแกนพอร์ต เซอร์วิส สแกนช่องโหว่ของระบบ โปรแกรมสำหรับเจาะระบบ เป็นต้น

หมวด ๑
นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดนโยบายและให้การสนับสนุนการจัดการเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ให้เป็นไปตามหรือสอดคล้องกับ กฎหมาย ระเบียบ และข้อกำหนดทางธุรกิจของ กฟภ.

แนวนโยบาย

๑) คณะกรรมการต้องประกาศนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งได้รับอนุมัติโดย ผวก. หรือผู้ที่ได้รับมอบหมาย ให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบและถือปฏิบัติ

๒) คณะกรรมการต้องติดตาม และประเมินผลการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง เพื่อเป็นข้อมูลในการพิจารณาปรับปรุงให้เหมาะสมกับสถานการณ์และการใช้งาน

หมวด ๒
การจัดโครงสร้างด้านความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์

เพื่อควบคุมและติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพย์สินสารสนเทศ สำหรับส่วนงานต่างๆ ภายใน กฟภ. รวมทั้งกำหนดแนวทางควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา และการปฏิบัติงานนอก กฟภ. ให้มีความมั่นคงปลอดภัย

แนวนโยบาย

๓) หน่วยงานที่รับผิดชอบงานบุคคลต้องกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่างๆ เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๔) เพื่อความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ผู้ใช้ต้องปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๕) ผู้รับผิดชอบสารสนเทศ ...

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

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

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

๘) ในการดำเนินงานทุกโครงการหรือทุกแผนงานต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

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

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

๑๑) คณะกรรมการมีหน้าที่ดูแลรับผิดชอบการจัดการ การสนับสนุนและกำหนดทิศทางการดำเนินงาน เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศที่ชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใดๆ

๑๒) คณะกรรมการต้องส่งเสริมให้เกิดความร่วมมือในการรักษาความมั่นคงปลอดภัยสารสนเทศในทุกภาคส่วนของ กฟภ.

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

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

๑๕) ผู้ดูแลระบบสารสนเทศต้องมีข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศสำหรับการอนุญาตให้ผู้ใช้ที่เป็นบุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของ กฟภ. ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๓ ...

หมวด ๓
ความมั่นคงปลอดภัยสารสนเทศด้านบุคลากร

วัตถุประสงค์

เพื่อวางกรอบการสรรหา การควบคุมและการติดตามบุคลากรที่เข้ามาปฏิบัติงานภายใน กฟภ. รวมถึงการจ้างบุคคลหรือหน่วยงานภายนอก การบริหารจัดการบุคลากรและผู้รับจ้างระหว่างการจ้างงาน เมื่อมีการเปลี่ยนแปลงหน้าที่การปฏิบัติงาน หรือเมื่อพ้นสภาพการเป็นพนักงานหรือลูกจ้าง เพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศ

แนวนโยบาย

๑๖) หน่วยงานที่รับผิดชอบงานบุคคลและหน่วยงานที่รับผิดชอบงานจ้างหรืองานโครงการที่มีการเข้าถึงทรัพย์สินสารสนเทศของ กฟภ. ต้องตรวจสอบคุณสมบัติและประวัติของผู้สมัครงานหรือคู่สัญญาจะต้องไม่มีประวัติการกระทำผิดกฎหมายสารสนเทศ การบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลสารสนเทศมาก่อน

๑๗) หน่วยงานด้านกฎหมายและบุคลากรของ กฟภ. ต้องระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศไว้ในสัญญา หรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก โดยให้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๘) ผู้บังคับบัญชาชั้นต้นขึ้นไปต้องกำกับดูแล และแจ้งให้พนักงานในสังกัดและบุคคลภายนอกถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

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

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

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

หมวด ๔ ...

หมวด ๔
การบริหารจัดการทรัพย์สินสารสนเทศ

วัตถุประสงค์

เพื่อบริหารจัดการทรัพย์สินสารสนเทศของ กฟภ. ให้ได้รับการปกป้องในระดับที่เหมาะสม ลดความเสี่ยงต่อการถูกเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต รวมถึงป้องกันการนำทรัพย์สินสารสนเทศไปใช้โดยผิดวัตถุประสงค์และเกิดความเสียหายกับทรัพย์สินสารสนเทศของ กฟภ.

แนวนโยบาย

๒๒) ทุกหน่วยงานต้องจัดเก็บทะเบียนทรัพย์สินสารสนเทศที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๒๓) ผู้บังคับบัญชาชั้นต้นขึ้นไปต้องกำหนดบุคคลดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศให้ชัดเจน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๒๔) ผู้ใช้ต้องใช้งานทรัพย์สินสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๒๕) ผู้ใช้ต้องส่งคืนทรัพย์สินสารสนเทศของ กฟภ. เมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญา หรือสิ้นสุดข้อตกลงการปฏิบัติงาน หรือสิ้นสุดการได้รับมอบหมายให้ใช้ระบบสารสนเทศให้กับ กฟภ. ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๒๖) หน่วยงานผู้รับผิดชอบสารสนเทศต้องจัดหมวดหมู่ข้อมูลสารสนเทศ กำหนดระดับความสำคัญและกำหนดชั้นความลับ เพื่อป้องกันข้อมูลสารสนเทศให้มีความปลอดภัย โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๒๗) ผู้รับผิดชอบสารสนเทศต้องจำแนกประเภทของข้อมูลสารสนเทศ และจัดการข้อมูลสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๒๘) เพื่อป้องกันข้อมูลถูกเปิดเผยหรือข้อมูลรั่วไหลโดยไม่ได้รับอนุญาต หรือการถูกนำไปใช้งานผิดวัตถุประสงค์ ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องจัดการและจัดเก็บข้อมูลสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๒๙) การบริหารจัดการสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ชนิดเคลื่อนย้ายได้ (Removable media) ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ ให้ผู้รับผิดชอบสารสนเทศและผู้ใช้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๓๐) การทำลายสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ชนิดเคลื่อนย้ายได้ (Removable media) ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ ให้ผู้รับผิดชอบสารสนเทศและผู้ใช้ถือปฏิบัติตามระเบียบ

คำสั่ง ...

คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๓๑) กรณีมีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูลสารสนเทศ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือถูกนำไปใช้ในทางที่ผิด หรืออุปกรณ์ หรือข้อมูลสารสนเทศได้รับความเสียหาย ให้ผู้รับผิดชอบสารสนเทศและผู้ใช้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๕
การควบคุมการเข้าถึง

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึง การใช้งานระบบสารสนเทศของ กฟภ. และการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกรวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่สารสนเทศของ กฟภ.

แนวนโยบาย

๓๒) ให้คณะกรรมการกำหนดและทบทวนนโยบายควบคุมการเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สอดคล้องกับกฎหมายหรือประกาศ และแจ้งให้ผู้ใช้รับทราบและถือปฏิบัติ

๓๓) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๓๔) ผู้ใช้ต้องมีบัญชีผู้ใช้เป็นของตนเอง และผู้รับผิดชอบสารสนเทศต้องมีเทคนิคการตรวจสอบตัวตนที่เพียงพอ เพื่อให้สามารถระบุตัวตนของผู้เข้าใช้งานระบบสารสนเทศได้ โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๓๕) ผู้รับผิดชอบสารสนเทศต้องจัดให้มีการลงทะเบียนบัญชีผู้ใช้ระบบสารสนเทศ และยกเลิกบัญชีผู้ใช้เพื่อควบคุมการให้สิทธิและการยกเลิกสิทธิในการเข้าใช้งานระบบสารสนเทศของ กฟภ. โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๓๖) เจ้าของระบบสารสนเทศต้องจำกัดจำนวน และควบคุมผู้มีสิทธิระดับสูง โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๓๗) ผู้ดูแลระบบสารสนเทศต้องกำหนดขั้นตอนการตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๓๘) หน่วยงานเจ้าของข้อมูลสารสนเทศต้องติดตามทบทวนระดับสิทธิในการเข้าถึงของผู้ใช้ตามรอบระยะเวลาที่ได้กำหนดไว้ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๓๙) หน่วยงาน ...

๓๙) หน่วยงานที่รับผิดชอบสารสนเทศต้องยกเลิกหรือเปลี่ยนแปลงสิทธิในการเข้าใช้งานระบบสารสนเทศของผู้ใช้ เมื่อได้รับแจ้งการยุติการจ้าง หรือการเปลี่ยนแปลงสภาพการจ้าง โยกย้ายหน่วยงาน การพักงาน ระงับการปฏิบัติหน้าที่ การปรับเปลี่ยนบุคลากร หรือการสิ้นสุดสัญญาจ้างของหน่วยงานภายนอก หรือบุคคลภายนอก หรืองานโครงการที่มีการเข้าถึงทรัพย์สินสารสนเทศของ กฟภ. เพื่อไม่ให้เกิดความเสียหายกับ กฟภ. ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๔๐) ผู้ใช้ต้องกำหนดรหัสผ่านในการเข้าถึงระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๔๑) หน่วยงานที่รับผิดชอบสารสนเทศต้องจำกัดการเข้าถึงข้อมูลสารสนเทศและฟังก์ชันต่างๆ ในแอพพลิเคชันของผู้ใช้และผู้ดูแลระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๔๒) ผู้ดูแลระบบสารสนเทศต้องกำหนดวิธีการ Log-on เข้าระบบปฏิบัติการคอมพิวเตอร์และระบบสารสนเทศ ให้เป็นไปอย่างปลอดภัย เพื่อป้องกันและควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๔๓) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ระบบสารสนเทศในความรับผิดชอบยุติการทำงาน (Session Time-Out) เมื่อว่างเว้นจากการใช้งาน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๔๔) ผู้ดูแลระบบสารสนเทศต้องจำกัดระยะเวลาการเชื่อมต่อกับระบบสารสนเทศที่มีระดับความเสี่ยงสูง เพื่อเพิ่มระดับการรักษาความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๔๕) ผู้รับผิดชอบสารสนเทศต้องออกแบบระบบบริหารจัดการรหัสผ่านที่สามารถทำงานแบบเชิงโต้ตอบกับผู้ใช้ (Interactive) และสามารถรองรับการกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๔๖) ผู้ดูแลระบบสารสนเทศต้องจำกัดการเข้าถึงการใช้งานโปรแกรมอรรถประโยชน์ต่างๆ อย่างเข้มงวด เนื่องจากโปรแกรมดังกล่าวอาจมีความสามารถควบคุมและเปลี่ยนแปลงการทำงานของระบบสารสนเทศได้ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๔๗) ผู้รับผิดชอบสารสนเทศต้องจำกัดการเข้าถึงซอร์สโค้ด (Source code) ของโปรแกรมโดยไม่ได้รับอนุญาต ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๔๘) ผู้ดูแลระบบสารสนเทศต้องจำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

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

ที่เกี่ยวกับ ...

ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๕๐) ผู้ดูแลระบบสารสนเทศต้องควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศทั้งทางกายภาพและระยะไกล ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๕๑) ผู้ดูแลระบบสารสนเทศต้องควบคุมเส้นทางการไหลของข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๕๒) คณะกรรมการต้องพิจารณากำหนดระบบสารสนเทศที่มีความสำคัญสูง ให้มีสภาพแวดล้อมที่แยกออกมาต่างหาก สำหรับกรณีที่มีความจำเป็นต้องใช้ระบบสารสนเทศร่วมกันระหว่างระบบงานให้มีการประเมินความเสี่ยงสำหรับการใช้งานนั้นๆ โดยให้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๕๓) ผู้รับผิดชอบสารสนเทศต้องกำหนดวิธีการตรวจสอบตัวตนของผู้ใช้ที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๖
การควบคุมการเข้ารหัสลับข้อมูล

วัตถุประสงค์

เพื่อให้การเข้ารหัสลับข้อมูลและการบริหารจัดการกุญแจเข้ารหัสลับ ทำให้ระบบสารสนเทศคงไว้ซึ่งการรักษาความลับของข้อมูลและป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

แนวนโยบาย

๕๔) คณะกรรมการต้องกำหนดมาตรฐานการเข้ารหัสลับข้อมูล ประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสมสำหรับข้อมูลที่จำเป็นต้องป้องกัน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๕๕) การบริหารจัดการกุญแจในการเข้ารหัส (Key Management) ให้ผู้รับผิดชอบสารสนเทศจัดทำแนวทางการบริหารจัดการกุญแจ (Key) เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของ กฟภ. ที่จำเป็นต้องมีกุญแจ (Key) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๗
ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศ การควบคุมการใช้งานและบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศ และอุปกรณ์สารสนเทศ ซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศของ กฟภ. ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

แนวนโยบาย ...

แนวนโยบาย

๕๖) ผู้บังคับบัญชาชั้นต้นขึ้นไปที่รับผิดชอบพื้นที่ต้องป้องกันขอบเขตพื้นที่ตั้งของหน่วยงาน (Security perimeter) ที่มีการติดตั้ง จัดเก็บ หรือใช้งานระบบสารสนเทศและข้อมูลสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๕๗) ผู้บังคับบัญชาชั้นต้นขึ้นไปที่ดูแลพื้นที่ที่ควบคุมต้องกำหนดให้มีบุคลากรกำกับดูแลการควบคุมการเข้าออกพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure area) โดยให้เฉพาะผู้มีสิทธิที่สามารถเข้าออกได้ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๕๘) ผู้บังคับบัญชาชั้นต้นขึ้นไปที่รับผิดชอบพื้นที่ต้องออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันและควบคุมการเข้าถึงสำนักงาน ห้องทำงาน พื้นที่ซึ่งมีข้อมูลสารสนเทศที่สำคัญ ห้องคอมพิวเตอร์ที่สำคัญ และพื้นที่ปฏิบัติงานของผู้รับผิดชอบสารสนเทศ หรืออุปกรณ์สารสนเทศต่างๆ

๕๙) คณะกรรมการต้องกำหนดแนวทางในการออกแบบและติดตั้งด้านกายภาพ เพื่อให้สามารถป้องกันภัยจากภายนอกในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๖๐) การทำงานในพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure area) ให้ผู้รับผิดชอบสารสนเทศและผู้ใช้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๖๑) ผู้บังคับบัญชาชั้นต้นขึ้นไปต้องควบคุมการเข้าถึงพื้นที่ที่ไม่ได้รับอนุญาต และกำหนดพื้นที่การรับส่งพัสดุ พื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าห้องคอมพิวเตอร์และควบคุมผู้ที่มาติดต่อไม่ให้เข้าถึงพื้นที่อื่นๆ ที่ไม่ได้รับอนุญาตหรือเข้าถึงระบบสารสนเทศได้

๖๒) ผู้รับผิดชอบสารสนเทศต้องกำหนดให้มีการจัดวางและป้องกันอุปกรณ์สารสนเทศให้เหมาะสมเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต โดยพิจารณาถึงความสำคัญของอุปกรณ์ เพื่อลดความเสี่ยงจากภัยธรรมชาติ หรืออันตรายต่างๆ จากภัยคุกคามที่มนุษย์ก่อขึ้น ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๖๓) ผู้รับผิดชอบสารสนเทศต้องกำหนดให้มีการป้องกันการหยุดชะงักของอุปกรณ์สารสนเทศที่อาจเกิดจากไฟฟ้าขัดข้อง (Power failure) หรือจากข้อผิดพลาดของระบบและอุปกรณ์ที่สนับสนุนการทำงานของระบบสารสนเทศ (Supporting utilities) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๖๔) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีการป้องกันความเสียหายและสัญญาณรบกวนของสายไฟฟ้า สายสื่อสาร รวมทั้งให้มีการป้องกันการดักรับสัญญาณ (Interception) ในช่องทางสื่อสาร

๖๕) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีการดูแลบำรุงรักษาอุปกรณ์สารสนเทศอย่างถูกวิธีเพื่อให้คงไว้ซึ่งสภาพความพร้อมใช้งานอยู่เสมอ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๖๖) การนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของ กฟภ. ให้ผู้รับผิดชอบสารสนเทศและผู้ใช้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๖๗) คณะกรรมการ ...

๖๗) คณะกรรมการต้องกำหนดมาตรการรักษาความปลอดภัยอุปกรณ์สารสนเทศของ กฟภ. และอุปกรณ์ส่วนตัวที่นำมาใช้ร่วมกับระบบสารสนเทศของ กฟภ. โดยให้คำนึงถึงความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานนอกสถานที่ปฏิบัติงานของ กฟภ.

๖๘) ก่อนการยกเลิกการใช้งานหรือการนำอุปกรณ์สารสนเทศและสื่อบันทึกข้อมูลที่ใช้ในการจัดเก็บข้อมูลสารสนเทศกลับมาใช้ใหม่ ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องมีการตรวจสอบว่าได้มีการลบ ย้าย หรือทำลาย ข้อมูลหรือซอฟต์แวร์ที่ติดตั้งไว้ด้วยวิธีการที่ไม่สามารถกู้คืนได้อีก โดยให้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๖๙) ผู้ใช้ต้องดูแลป้องกันเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด ที่อยู่ภายใต้ความดูแลรับผิดชอบของตนเองในระหว่างที่ไม่มีการใช้งาน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๗๐) คณะกรรมการต้องกำหนดนโยบายปราศจากข้อมูลสารสนเทศที่สำคัญบนโต๊ะทำงานและหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) เพื่อป้องกันการเปิดเผยข้อมูลสารสนเทศที่สำคัญจากบุคคลอื่น

หมวด ๘
ความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน

วัตถุประสงค์

เพื่อควบคุมให้การปฏิบัติงาน มีขั้นตอนที่ชัดเจน พร้อมใช้งาน และมีความมั่นคงปลอดภัยสารสนเทศ

แนวนโยบาย

๗๑) ผู้ดูแลระบบสารสนเทศต้องจัดทำ ปรับปรุง และดูแล เอกสารขั้นตอนการปฏิบัติงานที่เกี่ยวกับระบบสารสนเทศ ให้มีความถูกต้องเหมาะสม และให้อยู่ในสภาพพร้อมใช้งาน เพื่อใช้ในการปฏิบัติงาน

๗๒) กรณีที่มีการเปลี่ยนแปลงของระบบสารสนเทศให้ผู้รับผิดชอบสารสนเทศถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๗๓) ผู้รับผิดชอบสารสนเทศต้องติดตามและจัดทำแผนด้านทรัพยากรสารสนเทศเพื่อรองรับการปฏิบัติงานในอนาคตของ กฟภ. อย่างเหมาะสม ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๗๔) ผู้รับผิดชอบสารสนเทศต้องจัดให้การแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาต ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๗๕) ผู้รับผิดชอบสารสนเทศต้องควบคุม ตรวจสอบ ป้องกัน และกู้คืนระบบสารสนเทศจากโปรแกรมไม่พึงประสงค์ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๗๖) ผู้รับผิดชอบสารสนเทศ ...

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

๗๗) ผู้รับผิดชอบสารสนเทศต้องสำรองข้อมูลสารสนเทศ และทดสอบการนำข้อมูลสำรองกลับมาใช้งาน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๗๘) ผู้รับผิดชอบสารสนเทศต้องจัดให้มีการบันทึกกิจกรรมของผู้ใช้งานระบบสารสนเทศและเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่างๆ (Audit log) เพื่อประโยชน์ในการสืบสวน สอบสวนในอนาคต และเพื่อการติดตามการควบคุมการเข้าถึง ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๗๙) ผู้รับผิดชอบสารสนเทศต้องมีขั้นตอนการเฝ้าติดตาม และสังเกตการใช้งานระบบสารสนเทศ พร้อมทั้งให้มีการประเมินผลการติดตามสังเกตการใช้งานระบบสารสนเทศอย่างสม่ำเสมอ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๘๐) ผู้รับผิดชอบสารสนเทศต้องจัดเก็บและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับข้อผิดพลาด (Fault Log) ของระบบสารสนเทศอย่างสม่ำเสมอ และจัดการแก้ไขข้อผิดพลาดที่ตรวจพบอย่างเหมาะสม ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๘๑) ผู้รับผิดชอบสารสนเทศต้องป้องกันการแก้ไขข้อมูลการบันทึกกิจกรรมของผู้ใช้งานระบบสารสนเทศ และเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยต่างๆ (Audit log) รวมถึงข้อมูลที่เกี่ยวข้องกับข้อผิดพลาด (Fault Log) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๘๒) ผู้รับผิดชอบสารสนเทศต้องบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบสารสนเทศ (System administrator) และผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบ (System operator) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๘๓) ผู้ดูแลระบบสารสนเทศต้องควบคุมให้อุปกรณ์สารสนเทศ ระบบสารสนเทศของ กฟภ. ได้รับการตั้งเวลาให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้อง ตรงกับเวลาอ้างอิงสากล และต้องตรวจสอบเวลาของอุปกรณ์สารสนเทศ ระบบสารสนเทศของ กฟภ. รวมถึงปรับปรุงให้เป็นปัจจุบันเสมอ เพื่อป้องกันไม่ให้เกิดการบันทึกเวลาไม่ถูกต้อง

๘๔) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ.ที่ประกาศใช้ในปัจจุบัน

๘๕) ผู้รับผิดชอบสารสนเทศต้องบริหารจัดการช่องโหว่ทางเทคนิค ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๘๖) ผู้ดูแลระบบสารสนเทศต้องกำหนดสิทธิ์ให้ผู้ใช้ติดตั้งซอฟแวร์ได้เท่าที่จำเป็น ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๘๗) ผู้ตรวจสอบภายใน ...

๘๗) ผู้ตรวจสอบภายในของ กฟภ. ต้องทำแผนและข้อกำหนดการตรวจสอบ รวมถึงกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ โดยได้รับความเห็นชอบจากผู้รับผิดชอบสารสนเทศ เพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของกระบวนการทางธุรกิจ

๘๘) คณะกรรมการต้องกำหนดประเภทข้อมูลตามลำดับชั้นความลับเพื่อให้ผู้รับผิดชอบสารสนเทศและผู้ใช้ถือปฏิบัติตาม เพื่อเป็นการป้องกันไม่ให้มีการเข้าถึงข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) โดยไม่ได้รับอนุญาต

๘๙) คณะกรรมการต้องกำหนดนโยบายและขั้นตอนการปฏิบัติ เพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยน หรือใช้ข้อมูลร่วมกัน ผ่านระบบสารสนเทศที่มีการเชื่อมต่อระหว่างระบบสารสนเทศต่างๆ

หมวด ๙
ความมั่นคงปลอดภัยด้านเครือข่าย

วัตถุประสงค์

เพื่อควบคุมการบริหารจัดการเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอก กฟภ. รวมถึงการควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศกับหน่วยงานภายนอกให้มีความมั่นคงปลอดภัย

แนวนโยบาย

๙๐) ผู้ดูแลระบบสารสนเทศต้องบริหารจัดการ การควบคุมเครือข่ายคอมพิวเตอร์ เครือข่ายสื่อสาร เพื่อป้องกันภัยคุกคาม และมีการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและแอพพลิเคชันที่ทำงานบนเครือข่ายคอมพิวเตอร์ รวมทั้งข้อมูลสารสนเทศที่มีการแลกเปลี่ยนบนเครือข่าย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๙๑) ผู้ดูแลระบบสารสนเทศต้องควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายทั้งหมดลงในข้อตกลง หรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายใน หรือภายนอก

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

๙๓) ผู้รับผิดชอบสารสนเทศต้องควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๙๔) ผู้รับผิดชอบสารสนเทศต้องควบคุม และให้มีข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์ ทั้งที่เป็นการแลกเปลี่ยนระหว่างหน่วยงานภายใน กฟภ. และระหว่าง กฟภ. กับหน่วยงานภายนอก ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๙๕) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูล

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

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

หมวด ๑๐
ความมั่นคงปลอดภัยในการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์

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

แนวนโยบาย

๙๗) หน่วยงานที่มีการการจัดหาหรือจัดให้มีการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ต้องระบุความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบงานที่พัฒนาขึ้นมาใช้งานนับตั้งแต่เริ่มต้นออกแบบระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๙๘) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกงละเมิดสัญญา หรือมีการรั่วไหลหรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๙๙) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องป้องกันไม่ให้มีการแก้ไขเปลี่ยนแปลงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาตและรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ ที่มีการเผยแพร่ต่อสาธารณชนถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๐๐) เพื่อไม่ให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูลหรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยไม่ได้รับอนุญาต ให้หน่วยงานที่เกี่ยวข้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนที่มีการธุรกรรมทางออนไลน์ (Online transaction) ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๐๑) ผู้พัฒนาระบบสารสนเทศต้องพัฒนาซอฟต์แวร์และระบบสารสนเทศอย่างมั่นคงปลอดภัยตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๐๒) ผู้พัฒนาระบบสารสนเทศ ...

๑๐๒) ผู้พัฒนาระบบสารสนเทศต้องมีขั้นตอนการควบคุมการเปลี่ยนแปลงระบบสารสนเทศเป็นลายลักษณ์อักษร เพื่อควบคุมให้ระบบเป็นไปตามข้อตกลงที่กำหนดไว้และมีความมั่นคงปลอดภัยตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๐๓) กรณีมีการเปลี่ยนแปลงต่อระบบปฏิบัติการคอมพิวเตอร์ของระบบสารสนเทศ ให้ผู้พัฒนาระบบสารสนเทศทดสอบและทบทวนระบบสารสนเทศนั้น เพื่อให้มั่นใจได้ว่าไม่มีผลกระทบต่อการปฏิบัติงานกับระบบและด้านความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

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

๑๐๕) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องพัฒนาและติดตั้งใช้งานระบบสารสนเทศโดยคำนึงถึงหลักการความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๐๖) ผู้พัฒนาระบบสารสนเทศต้องกำหนดมาตรการป้องกันสภาพแวดล้อมการพัฒนาระบบอย่างมั่นคงปลอดภัยให้ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๐๗) เจ้าของระบบสารสนเทศต้องดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างช่วงพัฒนาซอฟต์แวร์ ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๐๘) ผู้พัฒนาระบบสารสนเทศต้องทดสอบด้านความมั่นคงปลอดภัยของระบบที่พัฒนาใหม่หรือระบบงานเดิมที่ปรับปรุง เพื่อให้แน่ใจว่าระบบสารสนเทศสามารถทำงานได้อย่างมั่นคงปลอดภัยตามความต้องการที่กำหนดไว้ โดยให้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๐๙) หน่วยงานที่เกี่ยวข้องต้องกำหนดให้มีเกณฑ์ในการตรวจรับระบบใหม่ หรือที่ปรับปรุงเพิ่มเติมทั้งที่มาจากการพัฒนาภายในองค์กร หรือที่มีการจัดหาจากจ้างพัฒนา และต้องทดสอบระบบก่อนที่จะนำระบบดังกล่าวมาใช้งานจริง โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

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

๑๑๑) ผู้พัฒนาระบบสารสนเทศต้องตรวจสอบ (Validate) ข้อมูลใดๆ ก่อนที่จะรับเข้าสู่แอพพลิเคชันเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม โดยถือปฏิบัติตามระเบียบ

คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๑๒) ผู้รับผิดชอบสารสนเทศต้องตรวจสอบ (Validate) การทำงานของแอพพลิเคชันเพื่อตรวจหาข้อผิดพลาดของข้อมูลที่อาจเกิดจากการทำงานหรือการประมวลผลที่ผิดพลาด โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๑๓) ผู้พัฒนาระบบสารสนเทศต้องรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอพพลิเคชัน เพื่อป้องกันและสร้างความมั่นใจว่าข้อมูลที่ได้รับจากการรับส่งข้อมูลเป็นข้อมูลที่ถูกต้องแท้จริง มาจากผู้ส่งที่ถูกต้อง และไม่ถูกแก้ไขระหว่างทางหรือถูกแก้ไขโดยผู้ไม่มีสิทธิ โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๑๔) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องร่วมกันดำเนินการให้มีการตรวจสอบ (Validate) ข้อมูลใดๆ อันเป็นผลจากการประมวลผลของแอพพลิเคชัน เพื่อให้มั่นใจได้ว่าข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๑๕) ผู้รับผิดชอบสารสนเทศต้องป้องกันการรั่วไหลของข้อมูลสารสนเทศ โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๑๑
การจัดการความสัมพันธ์กับผู้ให้บริการภายนอก

วัตถุประสงค์

เพื่อป้องกัน ควบคุม ติดตาม และตรวจสอบ การปฏิบัติงานของหน่วยงานผู้ให้บริการภายนอกให้มีประสิทธิภาพและมีความมั่นคงปลอดภัยสารสนเทศ

แนวนโยบาย

๑๑๖) ผู้รับผิดชอบสารสนเทศกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศในด้านต่างๆ เพื่อป้องกัน ควบคุม หรือบรรเทาความเสี่ยงจากผู้ให้บริการภายนอก ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๑๗) สำหรับข้อตกลงเพื่ออนุญาตให้บุคคลภายนอกเข้าถึงระบบสารสนเทศ หรือใช้ข้อมูลสารสนเทศของหน่วยงาน เพื่อการอ่าน การประมวลผล การบริหารจัดการระบบสารสนเทศ หรือการพัฒนาระบบสารสนเทศ ผู้รับผิดชอบสารสนเทศต้องระบุรายละเอียดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๑๘) ผู้รับผิดชอบสารสนเทศต้องควบคุมให้มีการกำหนดข้อตกลง และความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอก โดยให้ครอบคลุมถึงผู้ให้บริการภายนอกที่รับจ้างช่วงจากผู้ให้บริการภายนอกหลักเป็นผู้จัดหา

๑๑๙) ผู้รับผิดชอบสารสนเทศ ...

๑๑๙) ผู้รับผิดชอบสารสนเทศต้องติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของผู้ให้บริการภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๒๐) กรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน หน่วยงานที่เป็นคู่สัญญากับผู้ให้บริการภายนอกต้องประสานงานกับผู้ให้บริการภายนอกและให้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว โดยต้องรายงานให้ผู้บริหาร และผู้ที่เกี่ยวข้องรับทราบ รวมถึงให้กำหนดกระบวนการบริการจัดการความเสี่ยงดังกล่าวให้สอดคล้องเหมาะสมตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

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

หมวด ๑๒
การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

วัตถุประสงค์

เพื่อบริหารจัดการเหตุการณ์ไม่พึงประสงค์หรือไม่อาจคาดคิดด้านความมั่นคงปลอดภัยสารสนเทศให้ได้รับความเสียหายน้อยที่สุด จัดเก็บปัญหาที่เกิดขึ้น และเรียนรู้ข้อผิดพลาดมาปรับปรุงแก้ไขเพื่อป้องกันไม่ให้เกิดปัญหาซ้ำอีก

แนวนโยบาย

๑๒๒) คณะกรรมการต้องกำหนดขอบเขตความรับผิดชอบของการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๒๓) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ผ่านช่องทางที่เหมาะสมโดยเร็วที่สุด โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๒๔) ผู้ใช้ต้องบันทึกและรายงานจุดอ่อนใดๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๒๕) ผู้รับผิดชอบสารสนเทศต้องมีการประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด โดยให้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๒๖) ผู้รับผิดชอบสารสนเทศต้องมีมาตรการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๒๗) คณะกรรมการ ...

๑๒๗) คณะกรรมการต้องกำหนดวิธีการแยกประเภท การรวบรวมปริมาณ วิเคราะห์มูลค่าความเสียหายของเหตุขัดข้องด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น เพื่อใช้เป็นเกณฑ์วัดและการติดตามเพื่อใช้ในการเรียนรู้ในการดำเนินงานและลดโอกาสเกิดในอนาคต ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

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

หมวด ๑๓
การบริหารจัดการด้านการบริการ หรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

วัตถุประสงค์

เพื่อระบุเหตุการณ์ที่อาจทำให้การให้บริการสารสนเทศหยุดชะงัก การบริหารจัดการในภาวะฉุกเฉินที่มีการคำนึงถึงความมั่นคงปลอดภัยสารสนเทศ ให้บริการสารสนเทศดำเนินไปได้อย่างต่อเนื่อง

แนวนโยบาย

๑๒๙) ผู้รับผิดชอบสารสนเทศต้องระบุเหตุการณ์ใดๆ ที่อาจส่งผลให้การดำเนินงานหยุดชะงักและมีความเป็นไปได้ในการเกิดผลกระทบต่อเนื่องจากการหยุดชะงักนั้น ในแง่ของความมั่นคงปลอดภัยสารสนเทศ โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๓๐) ผู้รับผิดชอบสารสนเทศต้องจัดทำข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศที่จำเป็น โดยกำหนดให้เป็นส่วนหนึ่งของขั้นตอนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๓๑) ผู้รับผิดชอบสารสนเทศต้องกำหนดแผนกรณีมีเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงักเพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศ โดยคำนึงประเด็นความมั่นคงปลอดภัยสารสนเทศ และให้สอดคล้องกับกลยุทธ์ความต่อเนื่องทางธุรกิจ ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๓๒) คณะกรรมการต้องกำหนดกรอบงาน (Framework) สำหรับการพัฒนาแผนการบริหารจัดการเพื่อการดำเนินงานทางธุรกิจมีความต่อเนื่องในภาวะฉุกเฉิน โดยคำนึงประเด็นความมั่นคงปลอดภัยสารสนเทศและให้สอดคล้องกับกลยุทธ์ความต่อเนื่องทางธุรกิจ

๑๓๓) คณะกรรมการต้องจัดให้มีการฝึกซ้อม ทดสอบ และนำผลมาปรับปรุงแผนบริหารความต่อเนื่องให้เป็นปัจจุบันและมีประสิทธิผล

๑๓๔) ผู้รับผิดชอบสารสนเทศต้องประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งาน และต้องกำกับให้มีการติดตั้งระบบสารสนเทศสำรอง หรืออุปกรณ์สำรอง หรือระบบสำหรับสนับสนุนการให้บริการที่เพียงพอ เพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจที่เหมาะสม ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

หมวด ๑๔ ...

หมวด ๑๔
การปฏิบัติตามกฎระเบียบ

วัตถุประสงค์

เพื่อให้ผู้ใช้ปฏิบัติตาม รวมถึงให้มีการตรวจสอบการปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เพื่อให้การดำเนินงานของ กฟภ. เป็นไปตามกฎหมาย ระเบียบ ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยต่างๆ

แนวนโยบาย

๑๓๕) คณะกรรมการต้องรวบรวมกฎระเบียบ หลักเกณฑ์ และข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่มีความสอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่างๆ ของหน่วยงาน และจัดทำเป็นเอกสารเพื่อใช้เป็นข้อกำหนดในการปฏิบัติงานอย่างเป็นลายลักษณ์อักษร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๑๓๖) การใช้งานข้อมูลที่อาจถือเป็นทรัพย์สินทางปัญญาหรือการใช้งานซอฟต์แวร์มีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่างๆ ให้ผู้ใช้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

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

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

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

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

๑๔๑) ผู้บังคับบัญชาชั้นต้นขึ้นไปต้องกำกับดูแล ตรวจสอบ ให้พนักงานปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๔๒) ผู้รับผิดชอบสารสนเทศต้องทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๔๓) ผู้รับผิดชอบสารสนเทศต้องป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

๑๔๔) ผู้รับผิดชอบสารสนเทศ ...

๑๔๔) ผู้รับผิดชอบสารสนเทศต้องป้องกันการเข้าใช้งานเครื่องมือที่ใช้เพื่อการตรวจสอบเพื่อมิให้เกิดการใช้งานผิดประเภทหรือถูกละเมิดการใช้งาน (Compromise) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

ประกาศนี้ให้มีผลใช้บังคับตั้งแต่วันที่ ๒๐ ก.ค. ๒๕๖๑ เป็นต้นไป

ประกาศ ณ วันที่ ๒๐ ก.ค. ๒๕๖๑

(นายเสริมสกุล คล้ายแก้ว)
ผู้ว่าการการไฟฟ้าส่วนภูมิภาค