ผู้ว่าการ
วันที่ 8 ส.ค. 62 เวลา 11.เศษ
เลขที่รับ 11428

ฝ่ายสารสนเทศ
วันที่ 22 ก.ค. 2562
เลขรับที่ 2487
เวลา 11.21น.

สวก.(ทส)
เลขรับที่ 2919 วันที่ 24/7/62

การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

จาก คณะอนุกรรมการจัดทำนโยบายฯ ถึง ประธานกรรมการฯ (รผก.(ทส))
เลขที่ กมส.(มส) ๒๒๐ /๒๕๖๒ วันที่ 22 ก.ค. 2562
เรื่อง ขออนุมัติใช้นโยบายความมั่นคงปลอดภัยสารสนเทศ (ฉบับที่ ๒) พ.ศ. ๒๕๖๒ แนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๒ และขออนุมัติยกเลิกแนวปฏิบัติความมั่นคงปลอดภัยสำหรับสารสนเทศ พ.ศ. ๒๕๕๘ (ฉบับปรับปรุงครั้งที่ ๑)

เรียน ประธานกรรมการฯ (รผก.(ทส)) ผ่านเลขาฯ (อฝ.สท.)
23 ก.ค. 2562

๑. เรื่องเดิม

ตามอนุมัติ ผวก. ลงวันที่ ๒๐ กรกฎาคม ๒๕๖๑ เรื่อง ขออนุมัติยกเลิกนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ พ.ศ. ๒๕๕๘ และอนุมัติใช้นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ (เอกสารแนบ ๑) ในข้อ ๔.๔. และข้อ ๓.๒.๒. ให้ ฝสท., ฝคฟ., ฝวร., ฝมป., ฝสค., ฝพท. และ ฝวส. จัดทำ ปรับปรุง แก้ไข แนวปฏิบัติ วิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ ให้ครอบคลุมครบถ้วนถึงกิจกรรมและกระบวนงาน เพื่อให้สอดคล้องกับการทำงานหลักของแต่ละฝ่าย ตามแนวทางของนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ ให้แล้วเสร็จภายใน ๑๘๐ วัน นับถัดจากวันที่ ผวก. ลงนามสั่งการ และนำเสนอคณะอนุกรรมการจัดทำนโยบาย แนวปฏิบัติ วิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศพิจารณาให้แล้วเสร็จภายใน ๙๐ วัน เพื่อนำเสนอคณะกรรมการการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศพิจารณาต่อไป

๒. ข้อเท็จจริง

คณะอนุกรรมการฯ พิจารณาแล้วเห็นว่าเพื่อให้การดำเนินงานของ กฟภ. เป็นไปด้วยความเรียบร้อยและเป็นไปตามที่กฎหมายกำหนด คณะอนุกรรมการฯ จึงได้ดำเนินการคู่ขนานเพื่อจัดทำและรวบรวมแนวปฏิบัติ วิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศไปด้วย คณะอนุกรรมการฯ ได้เชิญหน่วยงานที่เกี่ยวข้องเข้าร่วมประชุมหารือเพื่อให้ได้ข้อมูลในการจัดทำแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศถูกต้องครบถ้วน โดยได้มีการร่วมประชุมหารือตามวันเวลา ดังนี้

วันที่	เดือน / ปี	เวลา
๙, ๑๓	กรกฎาคม ๒๕๖๑	๐๙.๓๐ – ๑๖.๓๐ น.
๑๗, ๒๙	สิงหาคม ๒๕๖๑	๐๙.๓๐ – ๑๖.๓๐ น.
๑๒, ๒๔	กันยายน ๒๕๖๑	๐๙.๓๐ – ๑๖.๓๐ น.
๒, ๒๔	ตุลาคม ๒๕๖๑	๐๙.๓๐ – ๑๖.๓๐ น.
๗, ๑๕	พฤศจิกายน ๒๕๖๑	๐๙.๓๐ – ๑๖.๓๐ น.
๓, ๑๙	ธันวาคม ๒๕๖๑	๐๙.๓๐ – ๑๖.๓๐ น.
๘, ๓๐	มกราคม ๒๕๖๒	๐๙.๓๐ – ๑๖.๓๐ น.
๑๘	กุมภาพันธ์ ๒๕๖๒	๐๙.๓๐ – ๑๖.๓๐ น.
๔, ๑๔, ๒๖	มีนาคม ๒๕๖๒	๐๙.๓๐ – ๑๖.๓๐ น.
๑๐	มิถุนายน ๒๕๖๒	๑๓.๓๐ – ๑๖.๓๐ น.

๒๖ ...

๒๖	มิถุนายน ๒๕๖๒	๑๓.๓๐ – ๑๖.๓๐ น.
๑๒	กรกฎาคม ๒๕๖๒	๐๙.๓๐ – ๑๒.๐๐ น.

๓. ข้อพิจารณา และการดำเนินการของคณะอนุกรรมการฯ

จากเรื่องเดิมและข้อเท็จจริงดังกล่าวข้างต้น คณะอนุกรรมการฯ ได้ร่วมพิจารณาและดำเนินการ ดังนี้

๓.๑ ปรับปรุง แก้ไข และจัดทำแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศเรียบร้อยแล้ว (เอกสารแนบ ๒) และเห็นควรยกเลิกแนวปฏิบัติความมั่นคงปลอดภัยสำหรับสารสนเทศ พ.ศ. ๒๕๕๘ (ฉบับปรับปรุงครั้งที่ ๑) เนื่องจากเนื้อหาตรงกับแนวทางปฏิบัติฯ ที่ได้มีการยกร่างใหม่ (เอกสารแนบ ๓)

๓.๒ ตามที่ได้มีการจัดทำแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๒ คณะอนุกรรมการฯ พิจารณาแล้วเห็นว่า ข้อความในข้อ ๑๐) ๑๓) ๑๙) ๒๐) ๒๕) ๒๖) ๒๙) ๓๘) ๓๙) ๔๑) ๖๐) ๖๑) ๗๖) ๘๘) ๑๐๗) ๑๑๖) ๑๓๐) ๑๓๖) และ ๑๔๐) ของนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ ไม่สอดสอดคล้องกับบทบาทหน้าที่และคำนิยาม จึงเห็นควรให้มีการแก้ไขข้อความของนโยบายความมั่นคงปลอดภัยสารสนเทศเดิม โดยจัดทำเป็นนโยบายความมั่นคงปลอดภัยสารสนเทศ (ฉบับที่ ๒) พ.ศ. ๒๕๖๒ เพิ่มเติม (เอกสารแนบ ๔)

๓.๓ ตามคำสั่งการไฟฟ้าส่วนภูมิภาค ที่ พ.(ก) ๘๗/๒๕๖๑ ลงวันที่ ๒๖ กุมภาพันธ์ ๒๕๖๑ (เอกสารแนบ ๕) รผก.(ทส) ได้แต่งตั้งคณะอนุกรรมการจัดทำนโยบาย แนวปฏิบัติ วิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อจัดทำนโยบาย แนวปฏิบัติฯ ซึ่งคณะอนุกรรมการฯ ได้ดำเนินการเรียบร้อยแล้ว ในส่วนวิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติการในการทำงานเห็นควรให้แต่ละหน่วยงานซึ่งทราบข้อมูลและรายละเอียดในการปฏิบัติงานตามภาระหน้าที่ของหน่วยงาน เป็นผู้จัดทำวิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติฯ โดยเพิ่มเนื้อหาเกี่ยวกับการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศฯ และแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศฯ ให้ครอบคลุม ครบถ้วน ถึงกิจกรรมและกระบวนงานในการทำงานหลักของหน่วยงาน

๔. ข้อเสนอ

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

๔.๑ อนุมัติใช้แนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๒ (เอกสารแนบ ๒) และให้ยกเลิกแนวปฏิบัติความมั่นคงปลอดภัยสำหรับสารสนเทศ พ.ศ. ๒๕๕๘ (ฉบับปรับปรุงครั้งที่ ๑) ตามข้อ ๓.๑ (เอกสารแนบ ๓)

๔.๒ อนุมัติใช้นโยบายความมั่นคงปลอดภัยสารสนเทศ (ฉบับที่ ๒) พ.ศ. ๒๕๖๒ ตามข้อ ๓.๒ (เอกสารแนบ ๔)

๔.๓ ลงนามในประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ (ฉบับที่ ๒) พ.ศ. ๒๕๖๒

๔.๔ ลงนามในแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๒

๔.๕ สั่งการให้แต่ละหน่วยงานเป็นผู้จัดทำวิธีปฏิบัติ คู่มือขั้นตอนปฏิบัติฯ โดยเพิ่มเนื้อหาเกี่ยวกับการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศฯ และแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศฯ ให้ครอบคลุม ครบถ้วน ถึงกิจกรรมและกระบวนงานในการทำงานหลักของหน่วยงาน และนำเสนอคณะกรรมการการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศให้ความเห็นชอบ ตามข้อ ๓.๓

จึงเรียน ...

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบขอได้โปรดนำเสนอ ผวก. เพื่อพิจารณาอนุมัติข้อ ๔.๑ ถึงข้อ ๔.๒ และลงนามข้อ ๔.๓ ถึงข้อ ๔.๔ พิจารณาสั่งการข้อ ๔.๕ ตามข้อเสนอต่อไป

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

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

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

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

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

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

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

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

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

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

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

ลงชื่อ............... อนุกรรมการ
(นายรังสิวุฒิ หมื่นยา)
วศก.๘ กผร.

ลงชื่อ............... อนุกรรมการ
(นายพศนน สัตพงศ์พันธุ์)
นตก.๕ กอก.(ก.๒)

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

-อนุมัติ ตามข้อ 4.1 - 4.2
-ลงนามแล้ว ตามข้อ 4.3-4.4
-สั่งการ ตามข้อ 4.5

(นายสมพงษ์ ปรีเปรม)
ผวก.
1 9 ส.ค. 2562

เรียน ผวก.

เพื่อโปรดพิจารณาอนุมัติข้อ 4.1 - 4.2 และลงนาม ข้อ 4.3 - 4.4 และพิจารณาสั่งการข้อ 4.5 ตามที่คณะอนุกรรมการจัดทำนโยบายฯ เสนอต่อไปด้วย

(นายชนาเศรษฐ์ พงษ์ทรงเสถียร)
รผก.(ทส)
-7 ส.ค. 2562

กมส.

(นายวินัย สิริโภคากร)
อฝ.สท.
2 0 ส.ค. 2562

กมส.(มส)
โทร.๖๑๓๕

รก.มส. - ทุกหมวก
- เพื่อทราบ
20 ส.ค. 2562

รก.มส.(วห) ผมส.
- ดำเนินการต่อไป
20 ส.ค. 2562

เลขที่รับเอกสาร 1 ฉบับ

การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

ประกาศการไฟฟ้าส่วนภูมิภาค
เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ
(ฉบับที่ ๒) พ.ศ. ๒๕๖๒

.....

โดยที่เห็นสมควรแก้ไขเพิ่มเติมประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ

อาศัยอำนาจตามความแห่งพระราชบัญญัติการไฟฟ้าส่วนภูมิภาค พ.ศ. ๒๕๐๓ ที่ใช้บังคับอยู่ในปัจจุบัน การไฟฟ้าส่วนภูมิภาค จึงวางนโยบายความมั่นคงปลอดภัยสารสนเทศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ (ฉบับที่ ๒) พ.ศ. ๒๕๖๒"

ข้อ ๒ ประกาศนี้ให้มีผลใช้บังคับนับแต่วันที่ประกาศเป็นต้นไป

ข้อ ๓ ให้ยกเลิกความใน ๑๐) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

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

ข้อ ๔ ให้ยกเลิกความใน ๑๓) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

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

ข้อ ๕ ให้ยกเลิกความใน ๑๙) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

"๑๙) หน่วยงานที่เกี่ยวข้องกับการฝึกอบรมต้องจัดอบรมและหรือผู้รับผิดชอบสารสนเทศต้องสื่อสารให้ผู้ใช้ทราบถึงนโยบายหรือระเบียบ หลักเกณฑ์ และวิธีปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่ กฟภ. ประกาศใช้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงเพื่อสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศในส่วนที่เกี่ยวข้องกับหน้าที่ความรับผิดชอบของตน"

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

"๒๐) การลงโทษผู้ใช้ที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ให้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน"

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

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

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

"๒๖) คณะกรรมการต้องจัดหมวดหมู่ข้อมูลสารสนเทศ กำหนดระดับความสำคัญ และกำหนดชั้นความลับ เพื่อป้องกันข้อมูลสารสนเทศให้มีความปลอดภัย โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน"

ข้อ ๙ ให้ยกเลิกความใน ๒๙) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

"๒๙) การบริหารจัดการสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ชนิดเคลื่อนย้ายได้ (Removable media) ของ กฟภ. ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ ให้ผู้รับผิดชอบสารสนเทศถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน"

ข้อ ๑๐ ให้ยกเลิกความใน ๓๘) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

"๓๘) หน่วยงานเจ้าของข้อมูลสารสนเทศต้องติดตามทบทวนสิทธิในการเข้าถึงของผู้ใช้ตามรอบระยะเวลาที่ได้กำหนดไว้ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน"

ข้อ ๑๑ ให้ยกเลิกความใน ๓๙) ของประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง นโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ และให้ใช้ความต่อไปนี้แทน

"๓๙) ผู้ดูแลระบบสารสนเทศต้องยกเลิกหรือเปลี่ยนแปลงสิทธิในการเข้าใช้งานระบบสารสนเทศของผู้ใช้ เมื่อได้รับแจ้งการยุติการจ้าง หรือการเปลี่ยนแปลงสภาพการจ้าง โยกย้ายหน่วยงาน การพักงาน ระงับการปฏิบัติหน้าที่ การปรับเปลี่ยนบุคลากร หรือการสิ้นสุดสัญญาจ้าง ตามข้อ ๒๑ หรือหน่วยงานผู้รับผิดชอบสารสนเทศเพื่อไม่ให้เกิดความเสียหายกับ กฟภ. ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน"

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

"๔๑) เจ้าของข้อมูลสารสนเทศต้องจำกัดการเข้าถึงข้อมูลสารสนเทศ และฟังก์ชันต่างๆ ในแอพพลิเคชันของผู้ใช้และผู้ดูแลระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน"

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

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

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

"๖๑) ผู้บังคับบัญชาชั้นต้นขึ้นไปที่รับผิดชอบพื้นที่ต้องควบคุมการเข้าถึงพื้นที่ที่ไม่ได้รับอนุญาตและกำหนดพื้นที่การรับส่งพัสดุ 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) หน่วยงานผู้รับผิดชอบสารสนเทศต้องป้องกันไม่ให้มีการเข้าถึงข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) โดยไม่ได้รับอนุญาต"

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

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

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

"๑๑๖) ผู้รับผิดชอบสารสนเทศต้องแจ้งให้ผู้ให้บริการภายนอกปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน"

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

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

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

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

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

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

ประกาศ ณ วันที่ ๑๙ ส.ค. ๒๕๖๒

(นายสมพงษ์ ปรีเปรม)
ผู้ว่าการการไฟฟ้าส่วนภูมิภาค

การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

แนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ
ประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๒

สารบัญ

		หน้า
คำนิยาม		๓
หมวด ๑	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ	๕
หมวด ๒	การจัดโครงสร้างด้านความมั่นคงปลอดภัยสารสนเทศ	๕
หมวด ๓	ความมั่นคงปลอดภัยสารสนเทศด้านบุคลากร	๑๐
หมวด ๔	การบริหารจัดการทรัพย์สินสารสนเทศ	๑๓
หมวด ๕	การควบคุมการเข้าถึง	๑๖
หมวด ๖	การควบคุมการเข้ารหัสลับข้อมูล	๒๖
หมวด ๗	ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม	๒๘
หมวด ๘	ความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน	๓๕
หมวด ๙	ความมั่นคงปลอดภัยด้านเครือข่าย	๔๗
หมวด ๑๐	ความมั่นคงปลอดภัยในการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ	๕๐
หมวด ๑๑	การจัดการความสัมพันธ์กับผู้ให้บริการภายนอก	๖๒
หมวด ๑๒	การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด	๖๔
หมวด ๑๓	การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง	๖๖
หมวด ๑๔	การปฏิบัติตามกฎระเบียบ	๖๙

แนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ
ประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๒

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" 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" หมายความว่า หน่วยงานที่ทำหน้าที่ในการจัดให้ได้มาซึ่งการพัฒนาระบบสารสนเทศให้กับหน่วยงาน

"ผู้รับผิดชอบสารสนเทศ" หมายความว่า เจ้าของระบบสารสนเทศ เจ้าของข้อมูลสารสนเทศ ผู้ดูแลระบบสารสนเทศ ผู้พัฒนาระบบสารสนเทศ

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

"ลายมือชื่ออิเล็กทรอนิกส์" หมายความว่า อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้น และเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

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

"อุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้" หมายความว่า แล็ปท็อปคอมพิวเตอร์ (Laptop Computer), สมาร์ทโฟน (Smartphone), แท็บเล็ต (Tablet) เป็นต้น

"สร้างความตระหนัก" หมายความว่า การทำให้ผู้ใช้ตระหนักและใช้อุปกรณ์สารสนเทศด้วยความระมัดระวัง เช่น หลังการเชื่อมกับระบบสารสนเทศของ กฟภ. ให้ทำการส่งข้อความไปแสดงบน สมาร์ทโฟน (Smartphone) ว่า ผู้ใช้ต้องไม่โพสต์ข้อความหมิ่นประมาทผู้อื่น เป็นต้น

"สื่อบันทึกข้อมูลอิเล็กทรอนิกส์ชนิดเคลื่อนย้ายได้ (Removable Media)" หมายความว่า Optical Media (CD/DVD), Tape Backup, Magnetic Media (Hard Disk และ External Hard Disk), Solid State Memory (USB Flash Drive, Memory Card , Solid State Drive) เป็นต้น

"วิธีการทางชีวภาพ (Authentication by Biometric traits)" หมายความว่า วิธีการที่ใช้ลายนิ้วมือ เรตินา ฝ่ามือ เสียง ในการพิสูจน์ตัวตน เป็นต้น

หมวด ๑
นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดนโยบายและให้การสนับสนุนการจัดการเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ให้เป็นไปตามหรือสอดคล้องกับ กฎหมาย ระเบียบ และข้อกำหนดทางธุรกิจของ กฟภ.

นโยบาย

๑) คณะกรรมการต้องประกาศนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งได้รับอนุมัติโดย ผวก. หรือผู้ที่ได้รับมอบหมาย ให้พนักงานและบุคคลภายนอกที่เกี่ยวข้องรับทราบและถือปฏิบัติ

๒) คณะกรรมการต้องติดตาม และประเมินผลการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง เพื่อเป็นข้อมูลในการพิจารณาปรับปรุงให้เหมาะสมกับสถานการณ์และการใช้งาน

หมวด ๒
การจัดโครงสร้างด้านความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์

เพื่อควบคุมและติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพย์สินสารสนเทศ สำหรับส่วนงานต่างๆ ภายใน กฟภ. รวมทั้งกำหนดแนวทางควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา และการปฏิบัติงานนอก กฟภ. ให้มีความมั่นคงปลอดภัย

นโยบาย

๓) หน่วยงานที่รับผิดชอบงานบุคคลต้องกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่างๆ เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศไว้อย่างชัดเจน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

หน่วยงานที่รับผิดชอบงานบุคคลควรปฏิบัติดังนี้

๓.๑ ร่วมมือกับหน่วยงานที่เกี่ยวข้องในการกำหนดเนื้องานหรือหน้าที่ความรับผิดชอบต่างๆ ของผู้ใช้ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

๓.๒ กำหนดตำแหน่งผู้มีอำนาจสูงสุดด้านความมั่นคงปลอดภัยของ กฟภ. โดยผู้มีอำนาจสูงสุดด้านความมั่นคงปลอดภัย ต้องมีบทบาทและหน้าที่ความรับผิดชอบในการกำหนดแผนงานหรือมาตรการด้านความมั่นคงปลอดภัยของ กฟภ.

๓.๓ กำหนดบทบาทและหน้าที่ความรับผิดชอบของผู้ใช้ในการดูแลและป้องกันทรัพย์สินสารสนเทศที่ตนใช้งานหรือถือครอง เช่น ฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์ต่อพ่วง หรืออื่นๆ

นโยบาย

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

แนวทางปฏิบัติ

ผู้ใช้ต้องปฏิบัติดังนี้

๔.๑ ปฏิบัติตามกิจกรรมหรือกระบวนการด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้

๔.๒ ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข ทำลาย หรือทำให้เสียหายต่อทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต

๔.๓ รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ความมั่นคงปลอดภัยที่พบไปยังหน่วยรับแจ้ง

๔.๔ ปฏิบัติงานตามหน้าที่ความรับผิดชอบของตนเองที่ได้กำหนดไว้

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๕.๑ กำหนดให้การปฏิบัติงานที่มีความสำคัญมีการแยกหน้าที่ความรับผิดชอบออกจากกันโดยมีผู้ปฏิบัติงานมากกว่าหนึ่งคนเพื่อป้องกันการทุจริตที่อาจเกิดขึ้นได้

๕.๒ กำหนดมาตรการเพื่อป้องกันการสมรู้ร่วมคิด

๕.๓ กำหนดให้มีการสอดส่องดูแลอย่างใกล้ชิดสำหรับงานที่มีความเสี่ยงต่อการเกิดความเสียหายกับ กฟภ. แม้ว่าจะมีการแยกหน้าที่ความรับผิดชอบออกจากกันแล้วก็ตาม

๕.๔ กำหนดให้มีการจัดเก็บหลักฐานที่สามารถใช้ตรวจสอบได้ในภายหลังสำหรับงานที่มีความเสี่ยงต่อการเกิดความเสียหายกับ กฟภ. แม้ว่าจะมีการแยกหน้าที่ความรับผิดชอบออกจากกันแล้วก็ตาม

๕.๕ กำหนดให้มีการตรวจสอบการแบ่งแยกหน้าที่ความรับผิดชอบออกจากกันอย่างสม่ำเสมอ

นโยบาย

๖) หน่วยงานของ กฟภ. ที่มีหน้าที่ติดต่อกับหน่วยงานภายนอกที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่างๆ ต้องกำหนดขั้นตอนและช่องทางในการติดต่อกับหน่วยงานภายนอกนั้นไว้อย่างชัดเจนตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

หน่วยงานของ กฟภ. ที่มีหน้าที่ติดต่อกับหน่วยงานภายนอกที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่างๆ ควรปฏิบัติดังนี้

๖.๑ กำหนดขั้นตอนในการติดต่อกับกับหน่วยงานภายนอกที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่างๆ เช่น สถานีตำรวจ สถานีดับเพลิง รถพยาบาล เป็นต้น

๖.๒ รวบรวมรายชื่อและช่องทางในการติดต่อกับหน่วยงานภายนอกที่ควบคุมดูแลสถานการณ์ฉุกเฉินภายใต้สถานการณ์ต่างๆ พร้อมทั้งปรับปรุงรายชื่อ และช่องทางในการติดต่อดังกล่าวให้เป็นปัจจุบัน

นโยบาย

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

แนวทางปฏิบัติ

ทุกสายงานของ กฟภ. ควรปฏิบัติดังนี้

๗.๑ กำหนดขั้นตอนในการติดต่อกับกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ เช่น สมาคม สมาพันธ์ บริษัทที่ปรึกษา เป็นต้น

๗.๒ รวบรวมรายชื่อและช่องทางในการติดต่อกับหน่วยงานภายนอกที่มีความเชี่ยวชาญเฉพาะด้านหรือหน่วยงานที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมทั้งปรับปรุงรายชื่อ และช่องทางในการติดต่อดังกล่าวให้เป็นปัจจุบัน

๗.๓ ใช้ความร่วมมือดังกล่าวเพื่อแลกเปลี่ยน ปรับปรุง หรือเรียนรู้ด้านความมั่นคงปลอดภัยเทคโนโลยี ผลิตภัณฑ์ ภัยคุกคาม จุดอ่อน หรือเรื่องอื่นๆ

๗.๔ แลกเปลี่ยนข้อมูลข่าวสารด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ เช่น การแจ้งเตือนเกี่ยวกับช่องโหว่ในระบบเทคโนโลยีสารสนเทศ การแจ้งเตือนเกี่ยวกับโปรแกรมอุดช่องโหว่ เป็นต้น

นโยบาย

๘) ในการดำเนินงานทุกโครงการหรือทุกแผนงานต้องคำนึงถึงความมั่นคงปลอดภัยสารสนเทศตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ทุกโครงการหรือทุกแผนงานควรปฏิบัติดังนี้

๘.๑ มีข้อกำหนดด้านความมั่นคงสารสนเทศอยู่ในวัตถุประสงค์ของทุกโครงการหรือทุกแผนงาน

๘.๒ ประเมินความเสี่ยงด้านความปลอดภัยของสารสนเทศ

๘.๓ กำหนดให้การรักษาความปลอดภัยของสารสนเทศเป็นส่วนหนึ่งของทุกโครงการหรือทุกแผนงาน

นโยบาย

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

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๙.๑ วิเคราะห์และประเมินความเสี่ยงในการใช้งานอุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้ที่เชื่อมกับระบบของ กฟภ.

๙.๒ สร้างความตระหนักเพื่อให้ผู้ใช้ระมัดระวังและป้องกันการใช้งานอุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้ที่เชื่อมกับระบบของ กฟภ.

๙.๓ กำหนดให้ผู้ใช้ระบุและพิสูจน์ตัวตนก่อนการเข้าถึง

๙.๔ กำหนดให้มีการควบคุม และตรวจสอบการใช้งานอุปกรณ์การสื่อสารที่เคลื่อนย้ายได้

๙.๕ กำหนดให้มีวิธีปฏิบัติในการป้องกันความเสี่ยงของอุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้ที่เชื่อมกับระบบของ กฟภ. เช่น ติดตั้งโปรแกรมป้องกันโปรแกรมประสงค์ร้ายที่ถูกต้องตามกฎหมาย เป็นต้น

๙.๖ เก็บข้อมูลจราจรทางคอมพิวเตอร์ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๙.๗ ห้ามผู้ใช้วางอุปกรณ์สารสนเทศหรืออุปกรณ์การสื่อสารที่เคลื่อนย้ายได้ที่เชื่อมกับระบบของ กฟภ. ในสถานที่ที่ไม่มีผู้ดูแล

นโยบาย

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

แนวทางปฏิบัติ

๑๐.๑ ผู้รับผิดชอบสารสนเทศควรกำหนดหลักปฏิบัติสำหรับการใช้งานจากภายนอกสำนักงาน (Teleworking) ดังนี้

๑ ชนิดของงานที่อนุญาตและไม่อนุญาตสำหรับการปฏิบัติงานจากระยะไกล

๒ ระบบงานหรือบริการต่างๆ ที่อนุญาตให้เข้าถึงได้จากระยะไกล

๓ ชั่วโมงหรือช่วงระยะเวลาการปฏิบัติงาน

๔ ชั้นความลับของข้อมูลที่อนุญาตให้เข้าถึงได้

๑๐.๒ ผู้ใช้ต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากเจ้าของระบบสารสนเทศ และต้องใช้งานตามระยะเวลาการเข้าถึงที่กำหนดไว้

๑๐.๓ ผู้รับผิดชอบสารสนเทศควรทำการพิสูจน์ตัวตนของผู้ใช้ก่อนเข้าใช้งาน

๑๐.๔ ผู้รับผิดชอบสารสนเทศควรกำหนดมาตรการให้ทรัพย์สินทางปัญญาที่เกิดขึ้นจากการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ถือเป็นทรัพย์สินของ กฟภ.

นโยบาย

๑๑) คณะกรรมการมีหน้าที่ดูแลรับผิดชอบการจัดการ การสนับสนุนและกำหนดทิศทางการดำเนินงาน เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศที่ชัดเจน ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใดๆ

นโยบาย

๑๒) คณะกรรมการต้องส่งเสริมให้เกิดความร่วมมือในการรักษาความมั่นคงปลอดภัยสารสนเทศในทุกภาคส่วนของ กฟภ.

นโยบาย

๑๓) ผู้ที่นำระบบสารสนเทศใหม่มาใช้ต้องพิจารณาทบทวน เพื่ออนุมัติการสร้าง การติดตั้งหรือการใช้งานในแง่มุมต่างๆ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ที่นำระบบสารสนเทศใหม่มาใช้ควรปฏิบัติดังนี้

๑๓.๑ มีกระบวนการอนุมัติการใช้งานระบบสารสนเทศใหม่

๑๓.๒ ควบคุมข้อกำหนดความต้องการของระบบสารสนเทศใหม่ให้ถูกต้องเหมาะสมและสอดคล้องกับนโยบาย มาตรฐานหรือข้อกำหนดด้านความมั่นคงปลอดภัย ของ กฟภ.

๑๓.๓ ตรวจสอบว่าระบบเทคโนโลยีสารสนเทศใหม่นั้นเป็นไปตามหรือสอดคล้องกับนโยบาย มาตรฐานหรือข้อกำหนดด้านความมั่นคงปลอดภัยของ กฟภ. ที่กำหนดไว้หรือไม่ และควรอนุมัติก็ต่อเมื่อเป็นไปตามนโยบาย มาตรฐาน และข้อกำหนดดังกล่าว

๑๓.๔ ตรวจสอบว่าฮาร์ดแวร์หรือซอฟต์แวร์ใหม่ที่ได้รับนั้นสามารถใช้งานและเข้ากันได้กับระบบงานปัจจุบันหรือไม่

นโยบาย

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

แนวทางปฏิบัติ

การอนุญาตให้หน่วยงานภายนอกหรือบุคคลภายนอกเข้าถึงระบบสารสนเทศหรือใช้ข้อมูลสารสนเทศของ กฟภ. ผู้รับผิดชอบสารสนเทศควรระบุความเสี่ยง ประเมินความเสี่ยงที่อาจเกิดขึ้น สามารถทำได้โดย กำหนดเหตุการณ์ความเสี่ยง โอกาสการเกิดขึ้นของเหตุการณ์ความเสี่ยง ระดับผลกระทบ และคำนวณค่าความเสี่ยงจากโอกาสและผลกระทบที่กำหนดนั้น

ในกรณีที่ค่าความเสี่ยงสูงเกินกว่าที่จะยอมรับได้ ควรกำหนดแนวทางป้องกัน เพื่อลดความเสี่ยงนั้น

นโยบาย

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

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๑๕.๑ กำหนดหน้าที่ความรับผิดชอบบุคคลภายนอก

๑๕.๒ แจ้งให้บุคคลภายนอกทราบว่า กฟภ. จะดำเนินการเฝ้าระวังและติดตามการใช้ระบบงานหรือบริการของบุคคลภายนอก อย่างสม่ำเสมอเพื่อป้องกันการใช้ผิดวัตถุประสงค์

๑๕.๓ กำหนดให้บุคคลภายนอกปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่เกี่ยวข้อง

หมวด ๓
ความมั่นคงปลอดภัยสารสนเทศด้านบุคลากร

วัตถุประสงค์

เพื่อวางกรอบการสรรหา การควบคุมและการติดตามบุคลากรที่เข้ามาปฏิบัติงานภายใน กฟภ. รวมถึงการจ้างบุคคลหรือหน่วยงานภายนอก การบริหารจัดการบุคลากรและผู้รับจ้างระหว่างการจ้างงาน เมื่อมีการเปลี่ยนแปลงหน้าที่การปฏิบัติงาน หรือเมื่อพ้นสภาพการเป็นพนักงานหรือลูกจ้าง เพื่อรักษาไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศ

นโยบาย

๑๖) หน่วยงานที่รับผิดชอบงานบุคคลหรือหน่วยงานที่รับผิดชอบงานจ้างหรืองานโครงการที่มีการเข้าถึงทรัพย์สินสารสนเทศของ กฟภ. ต้องตรวจสอบคุณสมบัติและประวัติของผู้สมัครงานหรือคู่สัญญาจะต้องไม่มีประวัติการกระทำผิดกฎหมายสารสนเทศ การบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลสารสนเทศมาก่อน

แนวทางปฏิบัติ

๑๖.๑ หน่วยงานที่รับผิดชอบงานบุคคลหรือหน่วยงานที่รับผิดชอบงานจ้างหรืองานโครงการที่มีการเข้าถึงทรัพย์สินสารสนเทศของ กฟภ. ควรตรวจสอบประวัติความเป็นมาของผู้สมัครงานหรือคู่สัญญาอย่างระมัดระวัง ไม่ให้ขัดต่อกฎหมาย ระเบียบ หรือข้อบังคับที่เกี่ยวข้องกับความเป็นส่วนบุคคล การจ้างงาน หรือแรงงาน

๑๖.๒ หน่วยงานที่รับผิดชอบงานบุคคลหรือหน่วยงานที่รับผิดชอบงานจ้างหรืองานโครงการที่มีการเข้าถึงทรัพย์สินสารสนเทศของ กฟภ. ควรตรวจสอบและให้คู่สัญญายืนยันความถูกต้องจากเอกสาร ข้อมูล หรือบุคคลอ้างอิงของผู้สมัครงานหรือคู่สัญญา

๑๖.๓ หน่วยงานที่รับผิดชอบงานบุคคลควรกำหนดขั้นตอนปฏิบัติสำหรับการตรวจสอบประวัติของผู้สมัครงาน และหน่วยงานที่รับผิดชอบงานจ้างหรืองานโครงการควรกำหนดขั้นตอนปฏิบัติสำหรับการตรวจสอบประวัติของคู่สัญญา

นโยบาย

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

แนวทางปฏิบัติ

หน่วยงานด้านกฎหมายและบุคลากรของ กฟภ. ควรระบุหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศไว้ในสัญญา หรือข้อตกลงการปฏิบัติงานของพนักงาน หรือสัญญาว่าจ้างหน่วยงานหรือบุคคลภายนอก โดยเนื้อหาต้องกำหนดให้มีการปฏิบัติตามระเบียบนโยบาย ข้อบังคับ ข้อกำหนดอื่นๆ ที่เกี่ยวข้อง

นโยบาย

๑๘) ผู้บังคับบัญชาชั้นต้นขึ้นไปต้องกำกับดูแล และแจ้งให้พนักงานในสังกัดและบุคคลภายนอกถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้บังคับบัญชาชั้นต้นขึ้นไปควรปฏิบัติดังนี้

๑๘.๑ แจ้งบทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย แก่พนักงานใหม่ในสังกัดและบุคคลภายนอกก่อนที่จะอนุญาตให้เริ่มต้นปฏิบัติงานกับ กฟภ.

๑๘.๒ กำกับดูแลการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศของพนักงานในสังกัดและบุคคลภายนอก

นโยบาย

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

แนวทางปฏิบัติ

หน่วยงานที่เกี่ยวข้องกับการฝึกอบรมและหรือผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๙.๑ กำหนดให้ผู้ใช้ทำการศึกษาและทำความเข้าใจนโยบายหรือระเบียบ หลักเกณฑ์ และวิธีปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่ กฟภ. ประกาศใช้เป็นปัจจุบัน

๑๙.๒ จัดให้มีการอบรมที่เกี่ยวข้องกับการปฏิบัติงานทั่วไปเพื่อให้ผู้ใช้ได้เรียนรู้และทำความเข้าใจในเรื่องดังต่อไปนี้ วิธีการใช้ระบบงาน วิธีการใช้งานซอฟต์แวร์สำเร็จรูป การแก้ปัญหาการใช้คอมพิวเตอร์เบื้องต้น การปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง เป็นต้น

๑๙.๓ จัดให้มีการอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัยเพื่อให้ผู้ใช้ได้เรียนรู้และทำความเข้าใจในเรื่องดังต่อไปนี้ นโยบายหรือระเบียบ หลักเกณฑ์ และวิธีปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่ กฟภ. ประกาศใช้เป็นปัจจุบัน ภัยคุกคามต่อความมั่นคงปลอดภัย ช่องทางและวิธีการรายงานเมื่อประสบกับเหตุการณ์ความมั่นคงปลอดภัย กระบวนการลงโทษเมื่อมีการฝ่าฝืนนโยบายความมั่นคงปลอดภัย เป็นต้น

นโยบาย

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

แนวทางปฏิบัติ

การลงโทษผู้ใช้ที่ฝ่าฝืนนโยบายหรือระเบียบปฏิบัติเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ให้เป็นไปตามระเบียบการไฟฟ้าส่วนภูมิภาคว่าด้วยการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ (ภาคผนวก ๑)

นโยบาย

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

แนวทางปฏิบัติ

หัวหน้าหน่วยงานที่รับผิดชอบงานบุคคล หรือหน่วยงานที่รับผิดชอบงานจ้างหรืองานโครงการที่มีการเข้าถึงทรัพย์สินสารสนเทศของ กฟภ. ควรมีการกำหนดขั้นตอนการแจ้งการยุติการจ้าง หรือการเปลี่ยนแปลงสภาพการจ้าง โยกย้ายหน่วยงาน การพักงาน ระงับการปฏิบัติหน้าที่ การปรับเปลี่ยนบุคลากร หรือการสิ้นสุดสัญญาจ้างของหน่วยงานภายนอกหรือบุคคลภายนอก หรืองานโครงการที่มีการเข้าถึงทรัพย์สินสารสนเทศของ กฟภ. ให้หน่วยงาน

ผู้รับผิดชอบสารสนเทศทราบ เพื่อดำเนินการยกเลิกหรือเปลี่ยนแปลงสิทธิการเข้าถึงระบบสารสนเทศทันที

หมวด ๔
การบริหารจัดการทรัพย์สินสารสนเทศ

วัตถุประสงค์

เพื่อบริหารจัดการทรัพย์สินสารสนเทศของ กฟภ. ให้ได้รับการปกป้องในระดับที่เหมาะสม ลดความเสี่ยงต่อการถูกเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต รวมถึงป้องกันการนำทรัพย์สินสารสนเทศไปใช้โดยผิดวัตถุประสงค์และเกิดความเสียหายกับทรัพย์สินสารสนเทศของ กฟภ.

นโยบาย

๒๒) ทุกหน่วยงานต้องจัดเก็บทะเบียนทรัพย์สินสารสนเทศที่จำเป็นในการค้นหา เพื่อการใช้งานในภายหลัง ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ทุกหน่วยงานควรจัดเก็บทะเบียนทรัพย์สินสารสนเทศที่จำเป็นในการค้นหา เพื่อการใช้งานในภายหลัง และให้มีการปรับปรุงทะเบียนทรัพย์สินสารสนเทศให้เป็นปัจจุบันอยู่เสมอ เช่น อุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์ อุปกรณ์สื่อสารและเครือข่าย ข้อมูลและเอกสาร เป็นต้น

นโยบาย

๒๓) ผู้บังคับบัญชาชั้นต้นขึ้นไปต้องกำหนดบุคคลดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศให้ชัดเจน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

๒๓.๑ หัวหน้าหน่วยงานตั้งแต่ผู้อำนวยการกองขึ้นไปควรกำหนดบุคคลดูแลควบคุมการใช้งานและรับผิดชอบทรัพย์สินสารสนเทศให้ชัดเจนในแต่ละรายการโดยจัดหมวดหมู่ของทรัพย์สินที่ตนเองถือครองตามหมวดต่างๆ เช่น หมวดอุปกรณ์คอมพิวเตอร์ หมวดซอฟต์แวร์ หมวดอุปกรณ์สื่อสารและเครือข่าย หมวดข้อมูลและเอกสาร เป็นต้น

๒๓.๒ โดยใครครอบครองอะไรก็ให้คนนั้นรับผิดชอบทรัพย์สินสารสนเทศนั้น ส่วนทรัพย์สินสารสนเทศส่วนกลางให้ผู้อำนวยการกองกำหนดบุคคลดูแล

นโยบาย

๒๔) ผู้ใช้ต้องใช้งานทรัพย์สินสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ใช้ต้องใช้งานทรัพย์สินสารสนเทศตามระเบียบการไฟฟ้าส่วนภูมิภาคว่าด้วยการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ (ภาคผนวก ๑)

นโยบาย

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

แนวทางปฏิบัติ

ผู้ใช้ที่ครอบครองทรัพย์สินสารสนเทศต้องส่งคืนทรัพย์สินสารสนเทศของ กฟภ. เมื่อสิ้นสุดสถานะการเป็นพนักงาน หรือสิ้นสุดสัญญา หรือสิ้นสุดข้อตกลงการปฏิบัติงาน หรือสิ้นสุดการได้รับมอบหมายให้ใช้ระบบสารสนเทศให้กับ กฟภ. ให้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

นโยบาย

๒๖) คณะกรรมการต้องจัดหมวดหมู่ข้อมูลสารสนเทศ กำหนดระดับความสำคัญ และกำหนดชั้นความลับ เพื่อป้องกันข้อมูลสารสนเทศให้มีความปลอดภัย โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

คณะกรรมการควรแต่งตั้งอนุกรรมการจากเจ้าของข้อมูลสารสนเทศ เพื่อจัดหมวดหมู่ข้อมูลสารสนเทศ กำหนดระดับความสำคัญ และกำหนดชั้นความลับ โดยพิจารณาจากลำดับความสำคัญเพื่อกำหนดแนวทางการควบคุมและป้องกันข้อมูลและประกาศใช้ โดยมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง

นโยบาย

๒๗) ผู้รับผิดชอบสารสนเทศต้องจำแนกประเภทของข้อมูลสารสนเทศ และจัดการข้อมูลสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรจำแนกประเภทของข้อมูลสารสนเทศ และจัดการข้อมูลสารสนเทศโดยมีแนวทางตามขั้นตอนปฏิบัติการจัดระดับชั้นข้อมูล (ภาคผนวก ๒)

นโยบาย

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

แนวทางปฏิบัติ

เพื่อป้องกันข้อมูลถูกเปิดเผยหรือข้อมูลรั่วไหลโดยไม่ได้รับอนุญาต หรือการถูกนำไปใช้งานผิดวัตถุประสงค์ ผู้รับผิดชอบสารสนเทศและผู้ใช้ควรจัดการและจัดเก็บข้อมูลสารสนเทศโดยมีแนวทางตามขั้นตอนปฏิบัติการจัดระดับชั้นข้อมูล (ภาคผนวก ๒)

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๒๙.๑ จัดทำขั้นตอนปฏิบัติสำหรับการบริหารจัดการสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ชนิดเคลื่อนย้ายได้ (Removable media) เช่น การลบหรือทำลายข้อมูล การจัดเก็บ การนำสื่อบันทึกข้อมูลสำคัญออกนอก กฟภ. การส่งสื่อบันทึกข้อมูลไปยังอีกสถานที่หนึ่ง การป้องกันการเสื่อมอายุ เป็นต้น

๒๙.๒ กำหนดให้มีมาตรการสำหรับการลบข้อมูลสำคัญในสื่อบันทึกข้อมูลเพื่อไม่ให้ผู้อื่นสามารถเข้าถึงข้อมูลนั้นได้อีก ก่อนที่จะทำลายหรือทิ้งสื่อบันทึกข้อมูลนั้นไป

๒๙.๓ จัดทำบัญชีรายชื่อของสื่อบันทึกข้อมูลสำคัญเพื่อป้องกันการสูญหาย

๒๙.๔ กำหนดให้มีการขออนุญาตก่อนที่จะนำสื่อบันทึกข้อมูลสำคัญออกนอก กฟภ. เช่น เทปในตู้ไลบรารี่สำหรับเก็บเทปของ กฟภ. เป็นต้น

๒๙.๕ กำหนดให้มีการลงบันทึกการนำสื่อบันทึกข้อมูลสำคัญไปใช้งานหรือออกนอก กฟภ.

๒๙.๖ กำหนดให้มีการจัดเก็บสื่อบันทึกข้อมูลสำคัญไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๒๙.๗ กำหนดให้มีการปฏิบัติตามข้อกำหนดหรือคำแนะนำจากผู้ผลิตที่เกี่ยวข้องกับการจัดเก็บสื่อบันทึกข้อมูล เช่น ไม่เก็บไว้ในสถานที่ที่มีอุณหภูมิสูง หรือมีสนามแม่เหล็กสูง

นโยบาย

๓๐) การทำลายสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ชนิดเคลื่อนย้ายได้ (Removable media) ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ ให้ผู้รับผิดชอบสารสนเทศและผู้ใช้ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศและผู้ใช้ควรทำลายสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ชนิดเคลื่อนย้ายได้ (Removable media) ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ อย่างมั่นคงปลอดภัย โดยมีแนวทางตามขั้นตอนปฏิบัติการทำลายสื่อบันทึกข้อมูล (ภาคผนวก ๓)

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๓๑.๑ ตรวจนับจำนวนอุปกรณ์ที่จัดเก็บข้อมูลสารสนเทศ ก่อนขนย้ายและเมื่อถึงปลายทาง เพื่อให้แน่ใจว่าขนย้ายครบถ้วน เพื่อป้องกันการศูนย์หาย หรือถูกนำไปใช้ในทางที่ผิด

๓๑.๒ ควบคุมการบรรจุเพื่อขนย้าย โดยต้องจัดเก็บอุปกรณ์ที่จัดเก็บข้อมูลสารสนเทศในที่บรรจุที่ปิดล็อค และกันกระแทก เพื่อให้แน่ใจว่าไม่ได้รับความเสียหายระหว่างการขนย้าย และป้องกันการเข้าถึงโดยบุคคลภายนอก

หมวด ๕
การควบคุมการเข้าถึง

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึง การใช้งานระบบสารสนเทศของ กฟภ. และการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกรวมถึงจากโปรแกรมที่ไม่พึงประสงค์ที่จะสร้างความเสียหายให้แก่สารสนเทศของ กฟภ.

นโยบาย

๓๒) ให้คณะกรรมการกำหนดและทบทวนนโยบายควบคุมการเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สอดคล้องกับกฎหมายหรือประกาศ และแจ้งให้ผู้ใช้รับทราบและถือปฏิบัติ

นโยบาย

๓๓) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรจำกัดให้ผู้ใช้สามารถเข้าถึงเฉพาะบริการทางเครือข่ายคอมพิวเตอร์ที่ตนเองได้รับอนุญาตให้ใช้ได้เท่านั้น โดยสิทธิที่ได้รับต้องเป็นไปตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๓๔.๑ กำหนดให้มีบัญชีผู้ใช้ในระบบงานแต่ละผู้ใช้ตามบทบาทความรับผิดชอบ และให้มีความแตกต่างกัน เช่น บัญชีของผู้ใช้ทั่วไป บัญชีของผู้ดูแลระบบสารสนเทศ เป็นต้น

๓๔.๒ ห้ามใช้บัญชีผู้ใช้ที่มีสิทธิในระดับสิทธิสูง เพื่อปฏิบัติงานทั่วไป

๓๔.๓ กำหนดให้มีการอนุมัติการใช้งานบัญชีผู้ใช้แบบกลุ่มอย่างเป็นลายลักษณ์อักษรเพื่อให้สามารถตรวจสอบได้ว่าใครคือผู้ใช้ของบัญชีแบบกลุ่มนี้บ้างและกำหนดให้ผู้ใช้เหล่านี้ต้องรับผิดชอบร่วมกันกรณีที่มีปัญหาเกิดขึ้น

๓๔.๔ กำหนดให้มีการใช้วิธีการทางเทคนิคสำหรับการพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัยสูงกับระบบงานที่มีความสำคัญสูงด้วยวิธีการทางชีวภาพหรือตามความเหมาะสม

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๓๕.๑ กำหนดขั้นตอนปฏิบัติสำหรับการเก็บทะเบียนผู้ใช้ระบบงานต่างๆ ดังนี้

๑ กำหนดให้มีการระบุชื่อบัญชีผู้ใช้แยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดชื่อบัญชีผู้ใช้ที่ซ้ำซ้อนกัน

๒ จำกัดการใช้งานบัญชีผู้ใช้แบบกลุ่มซึ่งมีการใช้งานร่วมกันภายใต้บัญชีเดียวกันและอนุญาตให้ใช้งานได้ก็ต่อเมื่อมีเหตุผลความจำเป็นในการใช้งาน

๓ กำหนดให้มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๔ กำหนดให้มีการบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบงานของผู้ใช้

๕ กำหนดให้มีการเพิกถอนสิทธิ์การเข้าถึงระบบงาน โดยอัตโนมัติ หรือทันที หรือภายในระยะเวลาที่กำหนดสำหรับรายบุคคล เมื่อผู้ใช้นั้นทำการลาออก เปลี่ยนตำแหน่งงาน หรือย้ายไปอยู่อีกหน่วยงาน

๖ กำหนดให้มีการตรวจสอบหรือทบทวนบัญชีผู้ใช้ระบบงานทั้งหมดอย่างเป็นสม่ำเสมอเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

๓๕.๒ กำหนดให้ผู้เป็นเจ้าของระบบสารสนเทศหรือผู้ที่ได้รับมอบหมายเท่านั้นทำหน้าที่เป็นผู้อนุมัติการเข้าถึงระบบงาน

๓๕.๓ กำหนดให้มีการให้สิทธิเข้าถึงโดยต้องระมัดระวังหรือคำนึงถึงการสมรู้ร่วมคิดกัน

๓๕.๔ ไม่อนุญาตการใช้ระบบงานแก่ผู้ร้องขอจนกว่าจะได้รับอนุมัติแล้วเท่านั้น

นโยบาย

๓๖) เจ้าของระบบสารสนเทศต้องจำกัดจำนวน และควบคุมผู้มีสิทธิระดับสูง โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

เจ้าของระบบสารสนเทศควรปฏิบัติดังนี้

๓๖.๑ จำกัดจำนวนและควบคุมผู้มีสิทธิระดับสูง ตามความจำเป็นในการใช้งาน และมีสิทธิตามบทบาทหน้าที่ที่ได้รับมอบหมาย

๓๖.๒ บันทึกการมอบหมายสิทธิของผู้มีสิทธิระดับสูง

นโยบาย

๓๗) ผู้ดูแลระบบสารสนเทศต้องกำหนดขั้นตอนการตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๓๗.๑ กำหนดให้รหัสผ่านมีความยาวไม่น้อยกว่า ๘ ตัวอักษร ต้องผสมกันระหว่างตัวเลข ตัวอักษร และสัญลักษณ์ต่างๆ

๓๗.๒ กำหนดให้ผู้ใช้เปลี่ยนรหัส อย่างสม่ำเสมอ และไม่ใช้รหัสผ่านเดิมที่เคยใช้แล้ว

๓๗.๓ กำหนดให้ผู้ใช้ต้องเปลี่ยนรหัสผ่านให้มีความยากต่อการเดา

๓๗.๔ กำหนดให้ระบบทำการตรวจสอบบัญชีผู้ใช้และรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนไปเป็นรหัสผ่านใหม่

๓๗.๕ กำหนดให้ผู้ใช้ต้องเก็บรักษารหัสผ่าน โดยถือว่าเป็นความลับเฉพาะบุคคล จะต้องไม่เปิดเผย และกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๓๗.๖ ตั้งรหัสผ่านชั่วคราวให้กับผู้ใช้ โดยต้องกำหนดรหัสผ่านชั่วคราวให้มีความยากต่อการเดาโดยผู้อื่น และต้องกำหนดรหัสผ่านเหล่านั้นให้มีความแตกต่างกัน

๓๗.๗ กำหนดให้ผู้ใช้ทำการเปลี่ยนรหัสผ่านโดยเร็วภายหลังจากที่ได้รับรหัสผ่านชั่วคราว

นโยบาย

๓๘) หน่วยงานเจ้าของข้อมูลสารสนเทศต้องติดตามทบทวนสิทธิในการเข้าถึงของผู้ใช้ตามรอบระยะเวลาที่ได้กำหนดไว้ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

หน่วยงานเจ้าของข้อมูลสารสนเทศควรปฏิบัติดังนี้

๓๘.๑ ติดตามทบทวนสิทธิในการเข้าถึงของผู้ใช้ทั่วไปตามรอบระยะเวลาที่ได้กำหนดไว้ เช่น ทบทวนระดับสิทธิทุกๆ ๖ เดือน หรือตามที่หน่วยงานเจ้าของข้อมูลสารสนเทศเป็นผู้พิจารณา

๓๘.๒ ทบทวนสิทธิของผู้ดูแลระบบสารสนเทศด้วยความถี่ที่มากกว่าผู้ใช้ทั่วไป เช่น ทบทวนระดับสิทธิทุกๆ ๓ เดือน หรือตามที่หน่วยงานเจ้าของข้อมูลสารสนเทศเป็นผู้พิจารณา

๓๘.๓ บันทึกการเปลี่ยนแปลงต่อบัญชีที่ได้ทำการทบทวนนั้น

นโยบาย

๓๙) ผู้ดูแลระบบสารสนเทศต้องยกเลิกหรือเปลี่ยนแปลงสิทธิในการเข้าใช้งานระบบสารสนเทศของผู้ใช้ เมื่อได้รับแจ้งการยุติการจ้าง หรือการเปลี่ยนแปลงสภาพการจ้าง โยกย้ายหน่วยงาน การพักงานระงับการปฏิบัติหน้าที่ การปรับเปลี่ยนบุคลากร หรือการสิ้นสุดสัญญาจ้าง ตามข้อ ๒๑ หรือหน่วยงานผู้รับผิดชอบสารสนเทศเพื่อไม่ให้เกิดความเสียหายกับ กฟภ. ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๓๙.๑ ดำเนินการเพิกถอนหรือเปลี่ยนรหัสผ่าน หรือเปลี่ยนสิทธิการเข้าถึงระบบงานของผู้ที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้

๓๙.๒ ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงทางกายภาพของผู้ที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้ เช่น การ scan นิ้วเพื่อผ่านประตู

๓๙.๓ ดำเนินการขอคืนกุญแจหรือบัตรสำหรับเข้าพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย (Secure area)

นโยบาย

๔๐) ผู้ใช้ต้องกำหนดรหัสผ่านในการเข้าถึงระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ใช้ควรปฏิบัติดังนี้

๔๐.๑ ตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำของตนเอง และเป็นรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

๔๐.๒ หลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยตัวอักขระที่เรียงกัน กลุ่มของตัวอักขระที่เหมือนกัน

๔๐.๓ เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผย

๔๐.๔ รหัสผ่านจะต้องมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยอาจผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวอักขระพิเศษ และสัญลักษณ์ต่างๆ

๔๐.๕ เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับครั้งแรกทันทีที่ทำการล็อกอินเข้าสู่ระบบงาน

๔๐.๖ ไม่กำหนดรหัสผ่านจากชื่อ ชื่อสกุลของผู้ใช้ ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตน คำศัพท์ที่ใช้ในพจนานุกรม หมายเลขโทรศัพท์

๔๐.๗ เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๔๐.๘ ผู้ดูแลระบบสารสนเทศควรทำการเปลี่ยนรหัสผ่านทุกๆ ๓ เดือน สำหรับผู้ใช้ทั่วไปควรทำการเปลี่ยนรหัสผ่าน ทุกๆ ๖ เดือน

๔๐.๙ ไม่กำหนดให้ระบบงานทำการบันทึกรหัสผ่านที่ใช้งาน

๔๐.๑๐ ไม่ใช้รหัสผ่านของตนร่วมกับผู้อื่น และไม่เปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น

๔๐.๑๑ เก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย และต้องไม่บันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น

นโยบาย

๔๑) เจ้าของข้อมูลสารสนเทศต้องจำกัดการเข้าถึงข้อมูลสารสนเทศ และฟังก์ชันต่างๆ ในแอพพลิเคชันของผู้ใช้และผู้ดูแลระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

๔๑.๑ เจ้าของข้อมูลสารสนเทศควรกำหนดให้มีการลงทะเบียนผู้ใช้และผู้ดูแลระบบสารสนเทศ เพื่อควบคุม จำกัดการเข้าถึงข้อมูลสารสนเทศและฟังก์ชันต่างๆ ในแอพพลิเคชัน เช่น การให้สิทธิในการอ่าน เขียน ลบ หรือสั่งให้โปรแกรมทำงาน

๔๑.๒ เจ้าของข้อมูลสารสนเทศควรกำหนดให้ผู้ใช้และผู้ดูแลระบบสารสนเทศ สามารถเข้าถึงได้เฉพาะข้อมูลสารสนเทศ และฟังก์ชันต่างๆ ที่จำเป็นต้องใช้งานเท่านั้น

นโยบาย

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

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๔๒.๑ ก่อนการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์และระบบสารสนเทศผู้ดูแลระบบสารสนเทศควรกำหนดให้ผู้ใช้ต้องใส่ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ที่ได้รับก่อนเข้าใช้งานทุกครั้ง

๔๒.๒ กำหนดให้จำกัดระยะเวลาในการป้อนรหัสผ่าน หรือจำนวนครั้งที่ผู้ใช้สามารถใส่ข้อมูลการ Log-on เข้าระบบ ผิดได้

๔๒.๓ กำหนดให้ไม่แสดงข้อความผิดพลาดจากการทำงาน ในลักษณะที่เปิดเผยข้อมูลภายในของระบบจนเกินความจำเป็น

๔๒.๔ กำหนดให้ส่งข้อความเตือนไปยังผู้ดูแลระบบสารสนเทศเพื่อเตือนให้ทราบว่ามีผู้ใช้พยายาม Log-on เข้าระบบ แต่ผิดพลาดเป็นจำนวนหลายครั้งแล้ว

๔๒.๕ บันทึกข้อมูลการ Log-on เข้าระบบปฏิบัติการคอมพิวเตอร์และระบบสารสนเทศทั้งที่สำเร็จและไม่สำเร็จ

นโยบาย

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

แนวทางปฏิบัติ

สำหรับผู้ใช้

๔๓.๑ ผู้ดูแลระบบสารสนเทศควรกำหนดให้ตัดและหมดเวลาการใช้งานในระยะเวลาที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง

๔๓.๒ ผู้ดูแลระบบสารสนเทศควรกำหนดให้ระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบเทคโนโลยีสารสนเทศอีกครั้ง หลังจากที่ระบบได้หมดเวลาการใช้งานไปแล้ว

๔๓.๓ ผู้ดูแลระบบสารสนเทศควรกำหนดให้ต้องตั้งค่าระยะเวลาการตอบสนองการเชื่อมต่อกับระบบสารสนเทศจากเครื่องปลายทาง หากไม่โต้ตอบเกิน ๑๐ นาที ระบบจะตัดการเชื่อมต่อโดยอัตโนมัติ

สำหรับบริหารจัดการระบบสารสนเทศและอุปกรณ์

๔๓.๔ ผู้ดูแลระบบสารสนเทศควรกำหนด Session Time-Out ของผู้ดูแลระบบสารสนเทศต้องไม่เกิน ๑๕ นาที กรณีต้องใช้งานเกิน ๑๕ นาที ต้องขออนุมัติจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

นโยบาย

๔๔) ผู้ดูแลระบบสารสนเทศต้องจำกัดระยะเวลาการเชื่อมต่อกับระบบสารสนเทศที่มีระดับความเสี่ยงสูง เพื่อเพิ่มระดับการรักษาความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๔๔.๑ กำหนดให้จำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน โดยให้ผู้ใช้สามารถใช้งานได้นานที่สุดภายในระยะเวลา ๓ ชั่วโมง ต่อการเชื่อมต่อ ๑ ครั้ง

๔๔.๒ กำหนดให้ ผู้ใช้สามารถงานได้เฉพาะในช่วงเวลาการทำงานตามปกติเท่านั้น หลังจากหมดช่วงเวลานี้ ระบบจะตัดการใช้งานทันที

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๔๕.๑ กำหนดให้จำกัดระยะเวลาในการป้อนรหัสผ่าน และหากผู้ใช้ป้อนรหัสผ่านผิดเกิน ๓ ครั้งในช่วงเวลาที่กำหนดระบบจะทำการล็อกสิทธิการเข้าถึงของผู้ใช้ ทำให้ผู้ใช้รายนั้นไม่สามารถเข้าถึงระบบปฏิบัติการได้อีก จนกว่าผู้ดูแลระบบสารสนเทศจะดำเนินการปลดล็อกให้

๔๕.๒ กำหนดให้ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีความพยายามเดารหัสผ่านจากเครื่องปลายทาง

๔๕.๓ กำหนดให้ผู้ใช้สามารถเปลี่ยนรหัสผ่านได้ด้วยตนเอง และต้องยืนยันรหัสผ่านใหม่ที่ตั้งอีกครั้ง

๔๕.๔ กำหนดให้ไม่แสดงข้อมูลรหัสผ่านของผู้ใช้บนหน้าจอในระหว่างที่ผู้ใช้กำลังใส่ข้อมูลรหัสผ่านของตนเอง

๔๕.๕ กำหนดให้จัดเก็บรหัสผ่านเดิมของผู้ใช้ไว้จำนวนหนึ่งเพื่อป้องกันการกลับไปใช้รหัสผ่านเดิมที่ได้เคยตั้งไปแล้ว

๔๕.๖ กำหนดให้จัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้แยกต่างหากจากข้อมูลของระบบงาน

นโยบาย

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

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๔๖.๑ กำหนดให้จัดทำบัญชีรายชื่อโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งานได้เท่านั้น เพื่อให้ผู้ดูแลระบบสารสนเทศใช้งานและไม่อนุญาตให้ผู้ใช้ทั่วไปสามารถใช้งานได้

๔๖.๒ ในกรณีที่ผู้ใช้ต้องการใช้งานโปรแกรมอรรถประโยชน์ ต้องแจ้งความจำเป็นในการขอใช้และทำการขออนุญาตจากผู้ดูแลระบบสารสนเทศ พร้อมระบุเหตุผลความต้องการใช้งาน โดยต้องลงนามเห็นชอบจากเจ้าของระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร

๔๖.๓ กำหนดให้แยกจัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน โดยแยกไว้ในไดเร็คทอรี่ต่างหากเพื่อให้ง่ายในการควบคุมและจัดการโปรแกรมเหล่านี้

๔๖.๔ กำหนดให้ยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์ที่ไม่มีความจำเป็นในการใช้แล้ว

๔๖.๕ กำหนดให้ต้องทำการตรวจสอบบันทึกการเรียกใช้งานอย่างสม่ำเสมอ

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๔๗.๑ กำหนดให้มีการจัดเก็บซอร์สโค้ดของระบบงานไว้ในไลบรารี่กลางสำหรับซอฟต์แวร์ของ กฟภ. เพื่อให้ง่ายในการบริหารจัดการและควบคุมการเข้าถึงไลบรารี่ดังกล่าว

๔๗.๒ กำหนดให้ไม่อนุญาตการจัดเก็บซอร์สโค้ดของระบบงานไว้บนเครื่องให้บริการ

๔๗.๓ กำหนดให้มีการควบคุมการเข้าถึงไลบรารี่สำหรับซอฟต์แวร์ของระบบงานโดยผู้ให้บริการภายนอก

๔๗.๔ กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารี่สำหรับซอฟต์แวร์ของระบบงานไว้ในสถานที่ที่มีความปลอดภัย

๔๗.๕ กำหนดให้มีการบันทึกข้อมูลล็อกแสดงกิจกรรมการเข้าถึงไลบรารี่ที่เก็บไฟล์ สำหรับซอฟต์แวร์ของระบบงาน เช่น รายละเอียดของการเปลี่ยนแปลงแก้ไขซอร์สโค้ด วัน เวลาที่นำซอฟต์แวร์ออกจากไลบรารี่ไปใช้งาน วันเวลาที่นำซอฟต์แวร์ที่ปรับปรุงใหม่มาจัดเก็บไว้ในไลบรารี่ เป็นต้น

นโยบาย

๔๘) ผู้ดูแลระบบสารสนเทศต้องจำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์ของหน่วยงานที่สามารถเข้าถึงได้จากภายนอก ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๔๘.๑ จำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้ตามวันที่ เวลา ช่วงเวลาที่ผู้รับผิดชอบสารสนเทศอนุญาตให้ใช้งาน

๔๘.๒ กำหนดให้ป้องกันหมายเลขเครือข่ายภายใน (IP Address) ของระบบเครือข่ายภายใน กฟภ. ไม่ให้หน่วยงานภายนอกมองเห็นได้

๔๘.๓ ติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System / Intrusion Detection System

นโยบาย

๔๙) ผู้ดูแลระบบสารสนเทศต้องระบุและตรวจสอบอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศโดยอัตโนมัติ (Automatic equipment identification) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๔๙.๑ กำหนดให้มีการใช้งานหมายเลขระบุอุปกรณ์คอมพิวเตอร์หรือเครือข่าย เพื่อบ่งชี้ว่าอุปกรณ์ที่ติดต่อหรือเชื่อมโยงเข้ามานั้นเป็นอุปกรณ์ที่ได้รับอนุญาตแล้วหรือไม่ เช่น การใช้หมายเลขเทอร์มินัล การใช้ MAC Address หรือใช้ไอพีแอดเดรส เป็นต้น

๔๙.๒ ระบุและตรวจสอบอุปกรณ์ที่เชื่อมต่อเข้ากับระบบสารสนเทศโดยอัตโนมัติ โดยใช้ไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่นๆ เพื่อใช้ในการกำหนดว่าหมายเลขระบุอุปกรณ์ใดจะสามารถเข้าถึงเครือข่ายส่วนใดของ กฟภ.

๔๙.๓ กำหนดให้มีการรักษาความมั่นคงปลอดภัยทางกายภาพต่ออุปกรณ์คอมพิวเตอร์หรือเครือข่าย เพื่อป้องกันการเปลี่ยนแปลงแก้ไขหมายเลขระบุอุปกรณ์เหล่านั้น

นโยบาย

๕๐) ผู้ดูแลระบบสารสนเทศต้องควบคุมการเข้าถึงช่องทางการดูแลระบบสารสนเทศทั้งทางกายภาพและระยะไกล ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๕๐.๑ กำหนดให้มีการใช้การล็อคด้วยกุญแจ เพื่อควบคุมการเข้าถึงทางกายภาพต่อพอร์ตของอุปกรณ์เครือข่าย เพื่อป้องกันการเข้าถึง ทางกายภาพ ต่ออุปกรณ์เหล่านั้น และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต เช่น ถ้ามีตู้ให้ทำการล็อคตู้ หรือล็อคประตูห้อง Server

๕๐.๒ ขออนุมัติจากผู้มีอำนาจก่อน ก่อนที่จะอนุญาตให้เข้าดำเนินการ บำรุงรักษาหรือบริหารจัดการ อุปกรณ์เครือข่าย จากระยะไกล

๕๐.๓ ยกเลิก หรือปิดพอร์ต บนอุปกรณ์เครือข่าย ที่ไม่มีความจำเป็นในการใช้งาน

๕๐.๔ ยกเลิก หรือปิดบริการ บนอุปกรณ์เครือข่าย ที่ไม่มีความจำเป็นในการใช้งาน

นโยบาย

๕๑) ผู้ดูแลระบบสารสนเทศต้องควบคุมเส้นทางการไหลของข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรใช้เกตเวย์หรืออุปกรณ์เครือข่าย เพื่อตรวจสอบไอพีแอดเดรสของทั้งต้นทางและปลายทาง และควบคุมเส้นทางการไหล ของข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์

นโยบาย

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

แนวทางปฏิบัติ

ให้คณะกรรมการพิจารณากำหนดระบบสารสนเทศที่มีความสำคัญสูง ให้มีสภาพแวดล้อมที่แยกออกมาต่างหาก สำหรับกรณีที่มีความจำเป็นต้องใช้ระบบสารสนเทศร่วมกันระหว่างระบบงานให้มีการประเมินความเสี่ยงสำหรับการใช้งานนั้นๆ ดังนี้

๕๒.๑ กำหนดให้ระบุระดับความสำคัญของระบบงาน ซึ่งไวต่อการรบกวน หรือมีผลกระทบสูงต่อองค์กร

๕๒.๒ กำหนดให้ติดตั้งระบบงานที่มีความสำคัญสูงแยกออกจากระบบงานทั่วไป ด้วยการแบ่งโซนปกติ หรือโซนสำหรับระบบงานที่มีความไวสูง

๕๒.๓ กำหนดให้ประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกันระหว่างระบบงานที่มีความสำคัญสูงกับระบบงานอื่นๆ ที่มีความสำคัญน้อยกว่า ตั้งแต่เริ่มโครงการ ระหว่างการใช้ทรัพยากรร่วมกัน รวมถึงให้กำหนดวิธีการตอบสนองต่อความเสี่ยงนั้นด้วย

๕๒.๔ กำหนดให้กำหนดหลักเกณฑ์การเข้าถึงระบบงานที่มีความสำคัญสูง หรือระบบงานที่ไวต่อการรบกวน

นโยบาย

๕๓) ผู้รับผิดชอบสารสนเทศต้องกำหนดวิธีการตรวจสอบตัวตนของผู้ใช้ที่เหมาะสมเพื่อควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๕๓.๑ กำหนดวิธีการตรวจสอบตัวตนของผู้ใช้ที่เหมาะสม เพื่อควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกล เช่น password หรือ USB Token

๕๓.๒ กำหนดให้ผู้ใช้ใช้เครือข่ายที่มีความมั่นคงปลอดภัย เช่น โดยผ่านระบบ VPN

หมวด ๖
การควบคุมการเข้ารหัสลับข้อมูล

วัตถุประสงค์

เพื่อให้การเข้ารหัสลับข้อมูลและการบริหารจัดการกุญแจเข้ารหัสลับ ทำให้ระบบสารสนเทศคงไว้ซึ่งการรักษาความลับของข้อมูลและป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

นโยบาย

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

แนวทางปฏิบัติ

ให้คณะกรรมการกำหนดมาตรฐานการเข้ารหัสลับข้อมูล ประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสมสำหรับข้อมูลที่จำเป็นต้องป้องกันดังนี้

๕๔.๑ กำหนดมาตรฐานการเข้ารหัสข้อมูลที่หน่วยงานนำมาใช้งาน โดยไม่อนุญาตให้ใช้การเข้ารหัสแบบเฉพาะตัว (Proprietary Encryption) ยกเว้นจะได้รับการรับรองจากหน่วยงานภายนอกที่เชื่อถือได้ว่าการเข้ารหัสแบบเฉพาะตัวเป็นวิธีการเข้ารหัสที่ปลอดภัย

๕๔.๒ ทำการประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสมสำหรับข้อมูลที่จำเป็นต้องป้องกัน

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๕๕.๑ กำหนดให้มีการบริหารจัดการกุญแจ สำหรับการเข้ารหัสข้อมูล เพื่อป้องกันการสูญหาย การเข้าถึง การเปิดเผย การทำลาย หรือการเปลี่ยนแปลงแก้ไขกุญแจโดยไม่ได้รับอนุญาต รวมทั้งกำหนดให้มีระบบสำหรับบริหารจัดการกุญแจดังกล่าว

๕๕.๒ กำหนดให้มีมาตรการทางกายภาพเพื่อป้องกันอุปกรณ์ที่ใช้ในการสร้างและจัดเก็บกุญแจสำหรับการเข้ารหัสข้อมูล

๕๕.๓ ระบบสำหรับการบริหารจัดการกุญแจ ควรอ้างอิงหรือสอดคล้องกับมาตรฐานสากลซึ่งเป็นที่ยอมรับและใช้ในการเข้ารหัสข้อมูล

๕๕.๔ ระบบสำหรับการบริหารจัดการกุญแจควรใช้วิธีการและขั้นตอนปฏิบัติที่มีความมั่นคงปลอดภัยเพื่อ

๑ สร้างกุญแจสำหรับการเข้ารหัสข้อมูล

๒ สร้างและแจกจ่ายใบรับรองอิเล็กทรอนิกส์ (Public key certificates)

๓ แจกจ่ายกุญแจให้กับผู้ใช้ รวมทั้งกำหนดขั้นตอนปฏิบัติสำหรับการเริ่มต้นใช้งานกุญแจเป็นครั้งแรกภายหลังจากที่ได้รับกุญแจ (Key activation)

๔ จัดเก็บกุญแจและกำหนดวิธีการในการเข้าถึงกุญแจ

๕ เปลี่ยนกุญแจใหม่ เช่น ในกรณีที่กุญแจเกิดการสูญหาย หรือถูกเปิดเผย

๖ กำหนดระยะเวลาการหมดอายุของกุญแจ

๗ จัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับกุญแจ เช่น กรณีที่กุญแจเกิดการสูญหาย ถูกเข้าถึง หรือถูกเปิดเผยโดยไม่ได้รับอนุญาต

๘ ยกเลิกกุญแจ เช่น เมื่อกุญแจถูกเข้าถึงหรือเปิดเผยโดยไม่ได้รับอนุญาต หรือเมื่อผู้ที่เป็นเจ้าของกุญแจลาออกจาก กฟภ.

๙ ทำลายกุญแจ

๑๐ จัดเก็บกุญแจเก่าไว้ชั่วระยะเวลาหนึ่ง (Key archival) ก่อนที่จะทำลาย

๑๑ กู้คืนกุญแจที่เกิดการสูญหายหรือถูกทำให้เสียหาย

๑๒ บันทึกและตรวจสอบกิจกรรมที่เกี่ยวข้องกับการบริหารจัดการกุญแจ เช่น กิจกรรมต่างๆ ในข้างต้น

๕๕.๕ กำหนดให้มีการใช้ใบรับรองอิเล็กทรอนิกส์เพื่อใช้ในการผูกผู้เป็นเจ้าของกุญแจเข้ากับใบรับรองอิเล็กทรอนิกส์นั้น

๕๕.๖ กำหนดให้การสร้างหรือการออกใบรับรองอิเล็กทรอนิกส์ มีการดำเนินการโดยผู้ให้บริการออกใบรับรองซึ่งเป็นที่รู้จักและเชื่อถือได้

๕๕.๗ กำหนดให้มีการตรวจสอบว่าผู้ให้บริการออกใบรับรองนั้นมีมาตรการและขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยที่เพียงพอหรือไม่

๕๕.๘ กำหนดให้มีการจัดทำสัญญาการให้บริการกับผู้ให้บริการภายนอกที่เกี่ยวข้องกับการบริหารจัดการกุญแจและการออกใบรับรองอิเล็กทรอนิกส์ สัญญาควรครอบคลุมถึงประเด็นดังนี้

๑ บริการที่ต้องการและรายละเอียด

๒ ระดับการให้บริการ เช่น ระยะเวลาการตอบสนองของผู้ให้บริการ เมื่อมีการติดต่อหรือร้องขอใช้บริการ

๓ หน้าที่ความรับผิดชอบของผู้ให้บริการ

๔ ความรับผิดชอบของผู้ให้บริการ เช่น กรณีที่กุญแจที่ส่งมาเกิดความเสียหายถูกเข้าถึงโดยไม่ได้รับอนุญาต

หมวด ๗
ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงทรัพย์สินสารสนเทศ การควบคุมการใช้งานและบำรุงรักษาด้านกายภาพของทรัพย์สินสารสนเทศ และอุปกรณ์สารสนเทศ ซึ่งเป็นโครงสร้างพื้นฐานที่สนับสนุนการทำงานของระบบสารสนเทศของ กฟภ. ให้อยู่ในสภาพที่มีความสมบูรณ์พร้อมใช้ รวมถึงป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

นโยบาย

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

แนวทางปฏิบัติ

ผู้บังคับบัญชาชั้นต้นขึ้นไปที่รับผิดชอบพื้นที่ควรปฏิบัติดังนี้

๕๖.๑ มีการจัดสภาพแวดล้อมทางกายภาพเพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ภายใน กฟภ. สภาพแวดล้อมทางกายภาพไม่ควรมีจุดอ่อนที่ผู้ไม่ประสงค์ดีสามารถใช้เป็นช่องทางในการบุกรุกเข้าสู่พื้นที่ภายใน กฟภ.

๕๖.๒ จัดให้มีการประเมินความเสี่ยงทางกายภาพและกำหนดมาตรการลดความเสี่ยง

๕๖.๓ ผนังล้อมรอบของสำนักงานหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในควรมีความแข็งแรง ทนทาน และปลอดภัยจากการถูกทุบ ทำลาย หรือทำให้เสียหาย

๕๖.๔ ประตูหรือทางเข้าสำนักงานหรืออาคารหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศควรจัดให้มีระบบเตือนภัยเพื่อป้องการการบุกรุกทางกายภาพ เช่น ประตูที่แน่นหนา ระบบควบคุมการเข้าออก กลไกการล็อคประตู

๕๖.๕ ดำเนินการติดตั้งระบบป้องกันการบุกรุกทางกายภาพสำหรับพื้นที่ที่มีความสำคัญ

๕๖.๖ กำหนดวิธีการตรวจตราประตู หน้าต่าง และประตูหนีไฟให้ล็อคอยู่เสมอเพื่อป้องกันการบุกรุกทางกายภาพ

๕๖.๗ หน้าต่างในบริเวณชั้นหนึ่งของพื้นที่ที่มีความสำคัญควรป้องกันการถูกทุบให้แตกหรือทำให้เสียหายเพื่อบุกรุกเข้ามาในพื้นที่สำคัญนั้น

๕๖.๘ จัดระบบการรักษาความปลอดภัย เช่น พนักงานรักษาความปลอดภัย (รปภ.) เพื่อควบคุมการเข้าออกของบุคคลภายนอก

๕๖.๙ ดำเนินการติดตั้งระบบป้องกันการบุกรุกทางกายภาพสำหรับพื้นที่ที่มีความสำคัญ

๕๖.๑๐ ดำเนินการตรวจสอบหรือทดสอบระบบป้องกันการบุกรุกทางกายภาพอย่างสม่ำเสมอเพื่อดูว่ายังใช้งานได้ตามปกติหรือไม่

นโยบาย

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

แนวทางปฏิบัติ

ผู้บังคับบัญชาชั้นต้นขึ้นไปที่ดูแลพื้นที่ที่ควบคุมควรปฏิบัติดังนี้

๕๗.๑ มีวิธีการการลงบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญ และจัดเก็บเพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๕๗.๒ กำหนดมาตรการการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้ลายนิ้วมือ เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ

๕๗.๓ กำหนดให้มีการสอดส่อง ดูแล และเฝ้าระวัง ผู้ให้บริการภายนอกที่มาปฏิบัติงาน ผู้ที่มาเยือน ในพื้นที่ หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายหรือเสียหายของทรัพย์สิน หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๕๗.๔ กำหนดเงื่อนไขการเข้าพื้นที่ หรือบริเวณที่มีความสำคัญ รวมถึงการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผล

๕๗.๕ กำหนดกลไกในการสร้างความตระหนักให้ผู้ที่มาเยือนเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติตามในระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๕๗.๖ กำหนดให้พนักงานหรือผู้รับการว่าจ้างหรือผู้มาเยือนติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการปฏิบัติงานและระยะเวลาที่อยู่ภายใน กฟภ.

๕๗.๗ กำหนดให้มีการสร้างความตระหนักเพื่อให้พนักงานแจ้ง รปภ. โดยทันทีที่พบเห็นบุคคลแปลกหน้าที่ไม่ติดบัตร

๕๗.๘ กำหนดให้มีการทบทวนหรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๕๗.๙ กำหนดให้ผู้รับผิดชอบสารสนเทศและผู้ใช้ปฏิบัติตามขั้นตอนปฏิบัติการควบคุมการเข้า-ออกพื้นที่ศูนย์คอมพิวเตอร์ (ภาคผนวก ๔) กรณีเข้า-ออกพื้นที่ศูนย์คอมพิวเตอร์

นโยบาย

๕๘) ผู้บังคับบัญชาชั้นต้นขึ้นไปที่รับผิดชอบพื้นที่ต้องออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันและควบคุมการเข้าถึงสำนักงาน ห้องทำงาน พื้นที่ซึ่งมีข้อมูลสารสนเทศที่สำคัญ ห้องคอมพิวเตอร์ที่สำคัญ และพื้นที่ปฏิบัติงานของผู้รับผิดชอบสารสนเทศ หรืออุปกรณ์สารสนเทศต่างๆ

แนวทางปฏิบัติ

ผู้บังคับบัญชาชั้นต้นขึ้นไปที่รับผิดชอบพื้นที่ควรออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพ เพื่อป้องกันและควบคุมการเข้าถึงโดยไม่ได้รับอนุญาต เช่น ติดตั้งที่ scan ลายนิ้วมือก่อนเข้าห้องคอมพิวเตอร์ที่สำคัญ

นโยบาย

๕๙) คณะกรรมการต้องกำหนดแนวทางในการออกแบบและติดตั้งด้านกายภาพ เพื่อให้สามารถป้องกันภัยจากภายนอกในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

นโยบาย

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

แนวทางปฏิบัติ

๖๐.๑ ผู้รับผิดชอบสารสนเทศควรกำหนดมาตรการควบคุมและดูแลการปฏิบัติงานของพนักงาน กฟภ. และผู้ให้บริการภายนอกที่มาปฏิบัติงานในพื้นที่หรือบริเวณสำคัญของ กฟภ. เช่น ห้ามการใช้อุปกรณ์ถ่ายภาพ วีดีโอ และเครื่องอัดเสียงภายในพื้นที่หรือบริเวณสำคัญของ กฟภ.

๖๐.๒ ผู้รับผิดชอบสารสนเทศควรปิดหรือล็อคพื้นที่หรือบริเวณสำคัญที่ไม่มีบุคลากรของ กฟภ. ดูแลอยู่ในบริเวณนั้น รวมทั้งสอดส่องดูแลพื้นที่ดังกล่าวอย่างต่อเนื่อง

๖๐.๓ กรณีใช้พื้นที่ศูนย์คอมพิวเตอร์ ให้ผู้รับผิดชอบสารสนเทศและผู้ใช้ปฏิบัติตามแนวทางปฏิบัติเรื่องการใช้พื้นที่ศูนย์คอมพิวเตอร์ (ภาคผนวก ๕)

นโยบาย

๖๑) ผู้บังคับบัญชาชั้นต้นขึ้นไปที่รับผิดชอบพื้นที่ต้องควบคุมการเข้าถึงพื้นที่ที่ไม่ได้รับอนุญาต และกำหนดพื้นที่การรับส่งพัสดุ พื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าห้องคอมพิวเตอร์ และควบคุมผู้ที่มาติดต่อไม่ให้เข้าถึงพื้นที่อื่นๆ ที่ไม่ได้รับอนุญาตหรือเข้าถึงระบบสารสนเทศได้

แนวทางปฏิบัติ

ผู้บังคับบัญชาชั้นต้นขึ้นไปที่รับผิดชอบพื้นที่ควรปฏิบัติดังนี้

๖๑.๑ กำหนดพื้นที่หรือบริเวณสำหรับการส่งมอบหรือขนถ่ายพัสดุเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๖๑.๒ กำหนดบุคลากรหรือผู้ที่สามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น ทั้งนี้เพื่อป้องกันการสูญหายหรือเสียหายของพัสดุที่มีการส่งมอบนั้น

๖๑.๓ กำหนดให้มีการตรวจสอบพัสดุหรือปัจจัยการผลิตที่มีการส่งมอบและอาจเป็นอันตรายต่อ กฟภ. ก่อนที่จะโอนย้ายพัสดุนั้นไปยังพื้นที่ที่จะมีการใช้งาน

๖๑.๔ กำหนดให้มีการลงทะเบียนและตรวจนับพัสดุที่มีการส่งมอบ

๖๑.๕ กำหนดกระบวนการสำหรับการรับส่งพัสดุขาเข้าและขาออกแยกออกจากกัน

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๖๒.๑ จัดวางอุปกรณ์คอมพิวเตอร์สำคัญ เช่น เซิร์ฟเวอร์ให้บริการ ไว้ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ดังกล่าวโดยพนักงานหรือบุคคลภายนอกอื่นให้น้อยที่สุด

๖๒.๒ กำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพ เพื่อลดความเสี่ยงจากการที่อุปกรณ์ถูกทำลาย ถูกทำให้เสียหายทางกายภาพ ถูกขโมย ถูกวางเพลิง ถูกทำให้เสียหายโดยวัตถุระเบิด การสั่นสะเทือน สิ่งสกปรก สารเคมีที่มีฤทธิ์ทำลายหรือกัดกร่อน รังสีแม่เหล็กไฟฟ้า การแทรกแซงโดยกระแสไฟฟ้าหรือคลื่นแม่เหล็ก น้ำ ฝุ่น ความร้อน และ/หรือ ความชื้น

๖๒.๓ กำหนดมาตรการป้องกันเพื่อไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศ

๖๒.๔ กำหนดให้มีการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบว่าระดับอุณหภูมิ ความชื้น อยู่ในระดับปกติหรือไม่

๖๒.๕ ออกแบบระบบเพื่อป้องกันฟ้าผ่าอาคารสำนักงาน และสายสัญญาณสื่อสารต่างๆ

๖๒.๖ กำหนดมาตรการป้องกันอุปกรณ์ไฟฟ้าเพื่อไม่ให้เกิดเสียหายจากการที่กระแสไฟฟ้าเกิน ไฟฟ้าตก หรือไฟฟ้ากระชาก

๖๒.๗ กำหนดมาตรการป้องกันอุปกรณ์คอมพิวเตอร์ที่มีการแพร่กระจายคลื่นแม่เหล็กไฟฟ้า ซึ่งจะมีการรั่วไหลของข้อมูลไปกับคลื่นแม่เหล็กไฟฟ้านั้น

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๖๓.๑ มีระบบสนับสนุนดังต่อไปนี้ที่เพียงพอต่อความต้องการใช้งานของระบบเทคโนโลยีสารสนเทศของ กฟภ.

๑ ระบบกระแสไฟฟ้า

๒ ระบบยูพีเอส

๓ เครื่องกำเนิดกระแสไฟฟ้าสำรองหรือวิธีการบริหารจัดการระบบไฟฟ้า หรือแผนสำรอง
๔ ระบบน้ำประปา
๕ ระบบให้ความร้อน
๖ ระบบระบายอากาศ
๗ ระบบปรับอากาศ
๘ ระบบสายสื่อสารสำรอง

๖๓.๒ มีการตรวจสอบหรือทดสอบระบบสนับสนุนดังกล่าวอย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าระบบยังทำงานได้ตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๖๓.๓ ใช้ระบบยูพีเอสเพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้ากับระบบเทคโนโลยีสารสนเทศที่สนับสนุนกระบวนการทางธุรกิจสำคัญ

๖๓.๔ กำหนดให้มีการทดสอบระบบยูพีเอสอย่างสม่ำเสมอโดยทดสอบให้ตรงตามคำแนะนำที่ผู้ผลิตได้ระบุไว้

๖๓.๕ มีแผนฉุกเฉินสำหรับระบบกระแสไฟฟ้า เช่น ในกรณีที่ระบบกระแสไฟฟ้าเกิดการล้มเหลวหรือดับ การเปิดใช้ระบบไฟฟ้าสำรองต้องทำอย่างไร เป็นต้น

๖๓.๖ จัดทำเครื่องกำเนิดกระแสไฟฟ้าสำรองเพื่อจ่ายไฟสำรองให้ในกรณีที่กระแสไฟฟ้าหลักเกิดการหยุดชะงักหรือดับเป็นระยะเวลายาวนาน

๖๓.๗ จัดเตรียมน้ำมันเชื้อเพลิงสำรองอย่างเพียงพอสำหรับเครื่องกำเนิดกระแสไฟฟ้าสำรองเพื่อเอาไว้ใช้งานในช่วงเกิดเหตุฉุกเฉิน

๖๓.๘ จัดให้มีระบบกระแสไฟฟ้าที่มีแหล่งจ่ายมากกว่าหนึ่งแหล่ง เพื่อสนับสนุนกระบวนการทางธุรกิจสำคัญ เช่น กรณีที่ไฟฟ้าจากแหล่งหนึ่งดับไปยังมีไฟฟ้าอีกแหล่งหนึ่งจ่ายสนับสนุนได้

๖๓.๙ จัดทำสวิตช์ฉุกเฉินไว้ใกล้กับบริเวณทางออกของห้องเครื่อง เพื่อให้สามารถปิดสวิตช์ดับอุปกรณ์ทั้งหมดได้โดยทันทีทันใดและอย่างรวดเร็ว

๖๓.๑๐ จัดทำระบบไฟส่องสว่างฉุกเฉินเพื่อรองรับในกรณีที่กระแสไฟฟ้าหลักเกิดการขัดข้องและต้องการแสงสว่างในพื้นที่หรือบริเวณต่างๆ

๖๓.๑๑ มีระบบจ่ายน้ำที่เพียงพอสำหรับระบบปรับอากาศที่ต้องใช้น้ำในการทำงาน

๖๓.๑๒ มีระบบจ่ายน้ำที่เพียงพอเพื่อสนับสนุนระบบดับเพลิงของอาคาร

๖๓.๑๓ มีการติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนในกรณีที่ระบบสนับสนุนการทำงานภายในห้องที่ติดตั้งระบบสนับสนุน ทำงานผิดปกติหรือหยุดการทำงาน

นโยบาย

๖๔) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีการป้องกันความเสียหายและสัญญาณรบกวนของสายไฟฟ้า สายสื่อสาร รวมทั้งให้มีการป้องกันการดักรับสัญญาณ (Interception) ในช่องทางสื่อสาร

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๖๔.๑ จัดให้มีการเดินสายไฟฟ้า สายสื่อสาร หรือสายสัญญาณอื่นๆ จากภายนอกอาคารผ่านลอดเข้ามาทางใต้ดิน

๖๔.๒ หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของ กฟภ. ในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกสามารถเข้าถึงได้

๖๔.๓ ให้มีการเดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการรบกวนของสัญญาณซึ่งกันและกัน

๖๔.๔ ให้มีการจัดทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์สื่อสารเพื่อให้สามารถค้นหาเส้นสายสัญญาณที่ต้องการได้โดยง่าย

๖๔.๕ ให้มีการจัดทำผังการเชื่อมต่อสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง รวมทั้งปรับปรุงให้ทันสมัยอยู่เสมอ

๖๔.๖ ให้มีการใช้งานสายไฟเบอร์ออฟติก สำหรับระบบเทคโนโลยีสารสนเทศที่มีความสำคัญ เพราะสายไฟเบอร์ออฟติกป้องกันการดักรับสัญญาณ (Interception) ได้ดีกว่าสายทองแดง

๖๔.๗ ให้มีการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดอย่างสม่ำเสมอเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสายสัญญาณโดยผู้ไม่ประสงค์ดี สำหรับระบบเทคโนโลยีสารสนเทศที่มีความสำคัญและบริเวณที่เป็นจุดเสี่ยง

นโยบาย

๖๕) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีการดูแลบำรุงรักษาอุปกรณ์สารสนเทศอย่างถูกวิธี เพื่อให้คงไว้ซึ่งสภาพความพร้อมใช้งานอยู่เสมอ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๖๕.๑ กำหนดให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๖๕.๒ กำหนดให้มีการปฏิบัติตามคำแนะนำในการบำรุงรักษาอุปกรณ์ตามที่ผู้ผลิตแนะนำหรือตามความเหมาะสม

๖๕.๓ กำหนดให้มีการจัดเก็บบันทึกกิจกรรม และปัญหารวมทั้งข้อบกพร่องของอุปกรณ์ที่พบในการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๖๕.๔ กำหนดให้มีการควบคุม สอดส่อง และดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายใน กฟภ.

๖๕.๕ กำหนดให้มีการควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่ ทั้งนี้เพื่อป้องกันการสูญหาย

๖๕.๖ การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้ให้บริการภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) ควรได้รับการอนุมัติโดยผู้มีอำนาจ

นโยบาย

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

แนวทางปฏิบัติ

๖๖.๑ ผู้ใช้ที่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของ กฟภ. ต้องได้รับการอนุมัติโดยผู้มีอำนาจ

๖๖.๒ ผู้รับผิดชอบสารสนเทศควรกำหนดระยะเวลาของการนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของ กฟภ.

๖๖.๓ ผู้รับผิดชอบสารสนเทศควรกำหนดให้มีการบันทึกข้อมูลการนำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของ กฟภ.

๖๖.๔ เมื่อมีการส่งคืน ผู้รับผิดชอบสารสนเทศควรกำหนดให้มีการตรวจสอบว่าระยะเวลาที่ส่งคืนตรงกับระยะเวลาที่อนุญาตไว้หรือไม่ และอุปกรณ์เกิดการชำรุดเสียหายหรือไม่

๖๖.๕ กรณีพื้นที่ศูนย์คอมพิวเตอร์ ให้ผู้รับผิดชอบสารสนเทศและผู้ใช้ปฏิบัติตามขั้นตอนปฏิบัติการควบคุมการเข้า-ออกพื้นที่ศูนย์คอมพิวเตอร์ (ภาคผนวก ๔)

นโยบาย

๖๗) คณะกรรมการต้องกำหนดมาตรการรักษาความปลอดภัยอุปกรณ์สารสนเทศของ กฟภ. และอุปกรณ์ส่วนตัวที่นำมาใช้ร่วมกับระบบสารสนเทศของ กฟภ. โดยให้คำนึงถึงความเสี่ยงที่แตกต่างกันจากการนำไปใช้งานนอกสถานที่ปฏิบัติงานของ กฟภ.

นโยบาย

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

แนวทางปฏิบัติ

ก่อนการยกเลิกการใช้งานหรือการนำอุปกรณ์สารสนเทศและสื่อบันทึกข้อมูลที่ใช้ในการจัดเก็บข้อมูลสารสนเทศกลับมาใช้ใหม่ ผู้รับผิดชอบสารสนเทศและผู้ใช้ควรมีการตรวจสอบว่าได้มีการลบ ย้าย หรือทำลาย ข้อมูลหรือซอฟต์แวร์ที่ติดตั้งไว้ด้วยวิธีการที่ไม่สามารถกู้คืนได้อีก โดยมีแนวทางตามขั้นตอนปฏิบัติการทำลายสื่อบันทึกข้อมูล (ภาคผนวก ๓)

นโยบาย

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

แนวทางปฏิบัติ

ผู้ใช้ต้องป้องกันเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด ที่อยู่ภายใต้ความดูแลรับผิดชอบของตนเองในระหว่างที่ไม่มีการใช้งาน ถูกเข้าถึงโดย

ไม่ได้รับอนุญาต เช่น ตั้งเวลา screen server, ทำการปิดหน้าจอเครื่องคอมพิวเตอร์เมื่อไม่อยู่ที่โต๊ะ, ตั้งรหัสผ่านของเครื่องคอมพิวเตอร์, ใส่รหัสผ่านทุกครั้งจึงจะสามารถเปิดหน้าจอเพื่อเข้าถึงเครื่องคอมพิวเตอร์หรือระบบงานได้, นำอุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด ใส่ลงในลิ้นชักที่มีกุญแจล็อค เป็นต้น

นโยบาย

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

แนวทางปฏิบัติ

ให้คณะกรรมการกำหนดนโยบายปราศจากข้อมูลสารสนเทศที่สำคัญบนโต๊ะทำงานและหน้าจอคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) เพื่อป้องกันการเปิดเผยข้อมูลสารสนเทศที่สำคัญจากบุคคลอื่นดังนี้

๗๐.๑ กำหนดให้ผู้ใช้ช่วยกันดูแลทรัพย์สินสารสนเทศส่วนกลางที่ใช้ร่วมกัน

๗๐.๒ กำหนดให้ผู้ใช้ดูแลทรัพย์สินสารสนเทศของหน่วยงานที่ตนเองใช้งาน ถือครองเสมือนเป็นทรัพย์สินสารสนเทศของตนเอง

๗๐.๓ กำหนดให้ผู้ใช้ต้องไม่ทิ้งทรัพย์สินสารสนเทศที่สำคัญ ให้อยู่ในสถานที่ที่ไม่ปลอดภัย

๗๐.๔ กำหนดให้ผู้ใช้เก็บเอกสาร ข้อมูลในการทำงาน สื่อบันทึกข้อมูล ไว้ในที่ปลอดภัย (ใส่ตู้ โต๊ะที่สามารถ ล็อกกุญแจได้)

๗๐.๕ กำหนดให้ผู้ใช้ต้องขออนุมัติจากผู้บังคับบัญชาก่อนทุกครั้ง กรณีที่ต้องการนำทรัพย์สินสารสนเทศต่างๆ ออกจากหน่วยงาน

๗๐.๖ กำหนดให้ผู้ใช้นำเอกสารสำคัญออกจากเครื่องพิมพ์โดยทันทีที่พิมพ์งานเสร็จ

๗๐.๗ กำหนดให้ผู้ใช้ปิดเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น

หมวด ๘
ความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน

วัตถุประสงค์

เพื่อควบคุมให้การปฏิบัติงาน มีขั้นตอนที่ชัดเจน พร้อมใช้งาน และมีความมั่นคงปลอดภัยสารสนเทศ

นโยบาย

๗๑) ผู้ดูแลระบบสารสนเทศต้องจัดทำ ปรับปรุง และดูแล เอกสารขั้นตอนการปฏิบัติงานที่เกี่ยวกับระบบสารสนเทศ ให้มีความถูกต้องเหมาะสม และให้อยู่ในสภาพพร้อมใช้งาน เพื่อใช้ในการปฏิบัติงาน

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๗๑.๑ จัดทำขั้นตอนปฏิบัติงานเป็นลายลักษณ์อักษรสำหรับกิจกรรมการปฏิบัติงานกับระบบเทคโนโลยีสารสนเทศ โดยได้รับความเห็นชอบจากผู้มีอำนาจ

๗๑.๒ จัดทำ ขั้นตอนปฏิบัติดังนี้ เป็นลายลักษณ์อักษร

๑ การปฏิบัติงานในศูนย์คอมพิวเตอร์

๒ การเปิดและปิดระบบงาน เช่น การเปิดเครื่อง ปิดเครื่อง เปิดระบบงาน ปิดระบบงานเปิดบริการ ปิดบริการ เป็นต้น

๓ การสำรองข้อมูล

๔ การบำรุงรักษาระบบและอุปกรณ์

๕ การบริหารจัดการระบบงาน

๖ การจัดการกับสื่อบันทึกข้อมูล เช่น การทำป้ายชื่อบ่งชี้ การลบ การป้องกันการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง เป็นต้น

๗ การส่งงานเข้าไปประมวลผลในเครื่องคอมพิวเตอร์ และการจัดการกับข้อผิดพลาดที่เกิดขึ้น

๘ การประมวลผลข้อมูล เช่น ขั้นตอนในการนำข้อมูลเข้าระบบงาน การประมวลผล และการแสดงผล เป็นต้น

๙ การใช้งานโปรแกรมยูทิลิตี้ (โปรแกรมที่จัดหามาหรือที่เป็นประเภทฟรีแวร์หรือแชร์แวร์ที่ได้มาทางอินเทอร์เน็ต และเป็นประโยชน์กับงานที่ปฏิบัติในลักษณะใดลักษณะหนึ่ง)

๑๐ การรายงานและการจัดการกับเหตุเสียที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๑๑ การจัดการกับการล้มเหลวของระบบเทคโนโลยีสารสนเทศ

๑๒ การกู้คืนระบบเทคโนโลยีสารสนเทศ

๑๓ การจัดการกับข้อมูลล็อกของระบบเทคโนโลยีสารสนเทศ

๗๑.๓ กำหนดให้มีผู้รับผิดชอบในการจัดทำเอกสารขั้นตอนปฏิบัติในข้างต้น และกำหนดให้มีการปรับปรุงเอกสารดังกล่าวอย่างสม่ำเสมอ

นโยบาย

๗๒) กรณีที่มีการเปลี่ยนแปลงของระบบสารสนเทศให้ผู้รับผิดชอบสารสนเทศถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

กรณีที่มีการเปลี่ยนแปลงของระบบสารสนเทศ ผู้รับผิดชอบสารสนเทศควรมีการควบคุมเพื่อป้องกันความเสี่ยงต่างๆ เช่น ความเสี่ยงที่ทำให้ระบบสารสนเทศไม่สามารถให้บริการได้ เป็นต้น

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๗๓.๑ ติดตามและจัดทำแผนด้านทรัพยากรสารสนเทศเพื่อรองรับการปฏิบัติงานในอนาคตของ กฟภ. เช่น วางแผนสำหรับปีถัดไป

๗๓.๒ แผนด้านขีดความสามารถของระบบเทคโนโลยีสารสนเทศควรพิจารณาปริมาณหรือแนวโน้มของความต้องการที่เพิ่มขึ้น และกำหนดความต้องการเพิ่มเติมเพื่อให้สอดคล้องกับปริมาณความต้องการที่เพิ่มขึ้นนั้น

๗๓.๓ วางแผนการจัดหาระบบเทคโนโลยีสารสนเทศโดยคำนึงถึงระยะเวลาที่จะได้รับระบบดังกล่าว เพื่อให้ทันกาลและทันต่อความต้องการใช้งาน

๗๓.๔ กำหนดให้มีการเฝ้าระวังและติดตามทรัพยากรของระบบเทคโนโลยีสารสนเทศอย่างต่อเนื่องเพื่อให้มีสภาพความพร้อมใช้งานและประสิทธิภาพที่เพียงพอต่อการใช้งานทั้งปัจจุบันและอนาคต

๗๓.๕ กำหนดให้มีการปรับแต่งระบบเทคโนโลยีสารสนเทศเพื่อปรับปรุงสภาพความพร้อมใช้งานและประสิทธิภาพให้ดียิ่งขึ้น

๗๓.๖ กำหนดค่าการใช้งานทรัพยากรของระบบเทคโนโลยีสารสนเทศขั้นต่ำสุด เช่น การใช้งานซีพียู หน่วยความจำ พื้นที่ดิสก์ เป็นต้น เพื่อให้มีการแจ้งเตือนหากระบบมีการใช้ทรัพยากรเกินกว่าค่าขั้นต่ำสุดที่กำหนดไว้นั้น

๗๓.๗ กำหนดให้มีการติดตามปริมาณการใช้งานทรัพยากรของระบบเทคโนโลยีสารสนเทศอย่างต่อเนื่องและเก็บผลการติดตามนั้นไว้เป็นข้อมูลแนวโน้มหรือสถิติการใช้งานทรัพยากรของระบบ

๗๓.๘ กำหนดให้มีการใช้ประโยชน์จากข้อมูลแนวโน้มการใช้ทรัพยากรของระบบเทคโนโลยีสารสนเทศเพื่อวางแผนปรับปรุง แก้ไข รวมทั้งกำหนดมาตรการป้องกันตามความจำเป็นสำหรับระบบเหล่านั้น

นโยบาย

๗๔) ผู้รับผิดชอบสารสนเทศต้องจัดให้การแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบและใช้งานจริงออกจากกัน เพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาต ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๗๔.๑ พิจารณาแยกระบบงานสำหรับการพัฒนา การทดสอบ และการใช้งานจริงออกจากกันตามความจำเป็น เพื่อป้องกันผลกระทบจากการทำงานของระบบงานหนึ่งที่มีต่ออีกระบบงานหนึ่ง ป้องกันการเข้าถึงข้อมูลบนเครื่องให้บริการโดยไม่ได้รับอนุญาต

๗๔.๒ กำหนดแนวทางสำหรับใช้ในการแยกระบบงานสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน

๗๔.๓ กำหนดให้มีมาตรการเพื่อควบคุมการถ่ายโอนระบบงานจากเครื่องที่ใช้สำหรับการพัฒนาไปสู่เครื่องที่ใช้สำหรับการใช้งานจริง

๗๔.๔ กำหนดให้มีการป้องกันการเข้าถึงซอฟต์แวร์ทูลและยูทิลิตี้ที่ใช้สำหรับการพัฒนาระบบงานโดยไม่ได้รับอนุญาต เช่น ผู้ที่ทำหน้าที่ติดตั้งบนเครื่องใช้งานจริงไม่ควรมีสิทธิในการเข้าถึงซอฟต์แวร์ทูลดังกล่าวบนเครื่องสำหรับการพัฒนา

๗๔.๕ กำหนดให้มีการติดตั้งระบบงานสำหรับการทดสอบให้เหมือนหรือใกล้เคียงกับระบบงานสำหรับใช้งานจริงให้มากที่สุด เพื่อให้สามารถค้นหาปัญหาที่เกิดขึ้นได้เร็วที่สุด ถ้าการทำงานของทั้งสองระบบงานได้ผลลัพธ์ไม่เหมือนกัน

๗๔.๖ กำหนดให้มีมาตรการป้องกันเพื่อไม่ให้มีการนำข้อมูลสำคัญ หรือข้อมูลที่เป็นความลับไปใช้ในการติดตั้งบนระบบสำหรับการทดสอบหรือพัฒนา

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๗๕.๑ มีมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของ กฟภ. เพื่อป้องกันการแพร่กระจายของโปรแกรมไม่พึงประสงค์ และควบคุมบุคคลภายนอกไม่ให้สามารถใช้งานระบบงานของ กฟภ. ได้

๗๕.๒ ห้ามการติดตั้งซอฟต์แวร์อื่นๆ ที่ กฟภ. ไม่อนุญาตให้ใช้งาน

๗๕.๓ ควบคุมการใช้ไฟล์หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก กฟภ.

๗๕.๔ กำหนดให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอเพื่อป้องกันโปรแกรมไม่พึงประสงค์ที่ติดมากับซอฟต์แวร์หรือข้อมูลนั้น

๗๕.๕ ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่พึงประสงค์ ในเครื่องคอมพิวเตอร์ที่ใช้งานของ กฟภ.

๗๕.๖ ทำการตรวจสอบโปรแกรมไม่พึงประสงค์ในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ เช่น สัปดาห์ละ ๑ ครั้ง

๗๕.๗ กำหนดให้ผู้ใช้ทำการตรวจสอบโปรแกรมไม่พึงประสงค์ในสื่อบันทึกข้อมูลที่ตนเองใช้งานอย่างสม่ำเสมอ เช่น บนซีดี ดีวีดี Thumb drive ที่มีการใช้งาน

๗๕.๘ กำหนดให้ผู้ใช้ทำการตรวจสอบโปรแกรมไม่พึงประสงค์ในข้อมูลที่จะนำมาใช้งาน ซึ่งรวมถึงข้อมูลที่ดาวน์โหลดมาใช้งานและไฟล์แนบที่ได้รับทางอีเมล์

๗๕.๙ ตรวจสอบโปรแกรมไม่พึงประสงค์บนเครื่องเซิร์ฟเวอร์ (Server) ที่ให้บริการต่างๆ ซึ่งรวมถึงเครื่องให้บริการอีเมล์ด้วย

๗๕.๑๐ จัดทำขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่พึงประสงค์ ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่พึงประสงค์ การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่พบ เป็นต้น

๗๕.๑๑ ติดตามและตรวจสอบข้อมูลข่าวสารที่เกี่ยวข้องกับโปรแกรมไม่พึงประสงค์อย่างสม่ำเสมอจากแหล่งที่เชื่อถือได้ เช่น thaisert

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๗๖.๑ กำหนดรายชื่อเว็บไซต์หรือรายชื่อระบบงานบนเว็บไซต์ที่อนุญาตให้ใช้งานโปรแกรมชนิดเคลื่อนที่ได้ (Mobile code)

๗๖.๒ กำหนดให้มีการใช้มาตรการทางเทคนิคที่เหมาะสมเพื่อควบคุมการทำงานของโปรแกรมชนิดเคลื่อนที่ได้ (Mobile code)

๗๖.๓ กำหนดให้มีการจำกัดการทำงานของโปรแกรมชนิดเคลื่อนที่ได้ (Mobile code) เพื่อให้สามารถเข้าถึงทรัพยากรของระบบได้ในวงจำกัด

๗๖.๔ กำหนดให้มีการอนุญาตการทำงานของโปรแกรมชนิดเคลื่อนที่ได้ (Mobile code) ในสภาวะแวดล้อมที่แยกต่างหาก

นโยบาย

๗๗) ผู้รับผิดชอบสารสนเทศต้องสำรองข้อมูลสารสนเทศ และทดสอบการนำข้อมูลสำรองกลับมาใช้งาน ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๗๗.๑ กำหนดชนิดของข้อมูลที่ต้องทำการสำรองเก็บไว้ ความถี่ในการสำรอง และผู้รับผิดชอบในการสำรองข้อมูล

๗๗.๒ ความถี่ในการสำรองข้อมูลควรสอดคล้องกับระยะเวลาที่ยอมรับได้หากข้อมูลนั้นจะไม่ได้รับการปรับปรุงให้เป็นข้อมูลล่าสุด เช่น ถ้าระยะเวลาที่ยอมรับได้มากที่สุดจะต้องไม่เกิน ๑ วัน การสำรองข้อมูลควรทำอย่างน้อยวันละ ๑ ครั้ง เป็นต้น

๗๗.๓ ชนิดและความถี่ในการสำรองข้อมูลควรสอดคล้องหรือสัมพันธ์กับความสำคัญของข้อมูลนั้น

๗๗.๔ กำหนดให้มีการบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น เพื่อเอาไว้ใช้ตรวจสอบในภายหลัง

๗๗.๕ กำหนดให้มีการจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่สำรอง (Backup site) ที่ใช้จัดเก็บข้อมูลสำรองกับตัว กฟภ. เองควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับ กฟภ. เช่น แผ่นดินไหว เป็นต้น

๗๗.๖ กำหนดให้มีมาตรการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่ มาตรการป้องกันสำหรับสถานที่สำรองควรเข้มแข็งเหมือนกับมาตรการที่ใช้กับสำนักงานหลัก (Main site)

๗๗.๗ กำหนดให้มีการทดสอบความเชื่อถือได้ของสื่อบันทึกข้อมูลสำรองอย่างสม่ำเสมอ กล่าวคือ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลบนสื่อบันทึกนั้นได้ตามปกติหรือไม่ เช่น ลองอ่านข้อมูลจากสื่อบันทึกข้อมูล

๗๗.๘ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๗๗.๙ กำหนดให้มีการทดสอบขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลนั้นอย่างสม่ำเสมอเพื่อดูว่าขั้นตอนที่กำหนดไว้ใช้ได้จริงหรือไม่

๗๗.๑๐ ขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลสำคัญ (ต่อกระบวนการทางธุรกิจ) ควรสามารถดำเนินการให้แล้วเสร็จได้ตามขั้นตอนภายในระยะเวลาเป้าหมายที่กำหนดไว้ (Recovery time objective)

๗๗.๑๑ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๗๗.๑๒ กำหนดให้มีการตรวจสอบว่าข้อมูลทั้งหมดของระบบงานสำคัญได้รับการสำรองไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ระบบ ซอฟต์แวร์สำหรับระบบงาน ข้อมูลคอนฟิกกูเรชัน ฐานข้อมูล เป็นต้น รวมทั้งมีความทันสมัยตามที่ต้องการ

๗๗.๑๓ กำหนดระยะเวลาสำหรับการจัดเก็บข้อมูลสำคัญแต่ละชนิด กล่าวคือ ต้องจัดเก็บข้อมูลไว้ให้ถึงตามระยะเวลาที่กำหนดไว้นั้น

๗๗.๑๔ กำหนดชนิดของข้อมูลสำคัญที่จะต้องมีการจัดเก็บไว้อย่างถาวร เช่น บันทึกจัดเก็บไว้ในเทปและไม่มีการลบทิ้ง

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๗๘.๑ ข้อมูลที่ควรกำหนดให้บันทึกไว้ ได้แก่

๑ ข้อมูลชื่อบัญชีผู้ใช้

๒ ข้อมูลวันเวลาที่เข้าถึงระบบ

๓ ข้อมูลวันเวลาที่ออกจากระบบ
๔ ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
๕ ข้อมูลชื่อเทอร์มินัล
๖ ข้อมูลสถานที่ของเทอร์มินัลที่ผู้ใช้ใช้งาน
๗ ข้อมูลการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ
๘ ข้อมูลความพยายามในการเข้าถึงทรัพยากรของระบบทั้งที่สำเร็จและไม่สำเร็จ เช่น การเข้าถึงไฟล์ต่างๆ ในระบบ
๙ ข้อมูลแสดงการเข้าถึงไฟล์ในลักษณะต่างๆ เช่น เปิด ปิด เขียน อ่าน เป็นต้น
๑๐ ข้อมูลการเปลี่ยนค่าคอนฟิกกูเรชันของระบบ
๑๑ ข้อมูลแสดงการใช้สิทธิ เช่น สิทธิของผู้ดูแลระบบสารสนเทศ
๑๒ ข้อมูลแสดงการใช้งานหรือเข้าถึงระบบงาน
๑๓ ข้อมูลไอพีแอดเดรสที่เข้าถึง
๑๔ ข้อมูลโพรโตคอลเครือข่ายที่ใช้
๑๕ ข้อมูลการแจ้งเตือนของระบบ
๑๖ ข้อมูลแสดงการหยุดการทำงานของระบบ
๑๗ ข้อมูลแสดงการสำรองข้อมูลทั้งที่สำเร็จและไม่สำเร็จ

๗๘.๒ ในกรณีที่ข้อมูลล็อกเป็นข้อมูลที่เกี่ยวข้องกับการบุกรุกระบบหรือเป็นข้อมูลส่วนบุคคล กฟภ. ควรกำหนดให้มีมาตรการที่เหมาะสมเพื่อป้องกันข้อมูลดังกล่าว

๗๘.๓ กำหนดมาตรการป้องกันเพื่อไม่ให้ผู้ดูแลระบบสารสนเทศสามารถลบหรือยกเลิกการเก็บข้อมูลล็อกซึ่งแสดงถึงกิจกรรมที่เกี่ยวข้องกับตนเอง

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๗๙.๑ มีขั้นตอนการเฝ้าติดตาม โดยให้ติดตาม
๑ ชื่อบัญชีผู้ใช้
๒ กิจกรรมการใช้งานและประเภทของกิจกรรม
๓ วัน/เวลาที่เข้าถึง
๔ ไฟล์หรือข้อมูลที่ถูกเข้าถึง
๕ โปรแกรมหรือยูทิลิตี้ที่ถูกเรียกใช้งาน

๗๙.๒ มีการประเมินความเสี่ยงสำหรับระบบเทคโนโลยีสารสนเทศที่ใช้งานเพื่อกำหนดแนวทางในการเฝ้าระวังและดูแลระบบเหล่านั้น

๗๙.๓ กำหนดให้มีการเฝ้าระวังและตรวจสอบระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่ กฟภ. ต้องปฏิบัติตาม

๗๙.๔ กำหนดให้มีการเฝ้าระวังและตรวจสอบการเข้าถึงระบบเทคโนโลยีสารสนเทศที่ใช้สิทธิในระดับสูงอย่างสม่ำเสมอ การตรวจสอบสามารถดูได้จากข้อมูลล็อก เช่น ข้อมูล

๑ การใช้บัญชีผู้ใช้ในระดับสูง เช่น supervisor, root, administrator เป็นต้น เพื่อปฏิบัติงาน

๒ การเปิด-ปิดการทำงานของระบบหรืออุปกรณ์สำคัญ

๓ การถอดถอนหรือติดตั้งอุปกรณ์อินพุทและเอ้าพุท (เช่น ฮาร์ดดิสก์)

๗๙.๕ กำหนดให้มีการเฝ้าระวังและตรวจสอบการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต การตรวจสอบสามารถดูได้จากข้อมูลล็อก เช่น ข้อมูล

๑ การใช้คำสั่งบางอย่างที่ได้รับการปฏิเสธโดยระบบ เช่น การพยายามเข้าถึงและใช้คำสั่งนั้นทั้งที่ไม่มีสิทธิ

๒ ความพยายามในการเข้าถึงข้อมูลหรือทรัพยากรของระบบซ้ำหลายๆ ครั้ง

๓ ความพยายามในการเข้าถึงข้อมูลหรือทรัพยากรแต่ได้รับการปฏิเสธโดยระบบ

๔ การแจ้งเตือนจากไฟร์วอลล์หรือระบบป้องกันการบุกรุก

๗๙.๖ กำหนดให้มีการเฝ้าระวังและตรวจสอบการแจ้งเตือนหรือการล้มเหลวในการทำงานของระบบเทคโนโลยีสารสนเทศ การตรวจสอบสามารถดูได้จากข้อมูลล็อก เช่น ข้อมูล

๑ การแจ้งเตือนจากคอนโซล (console) ของผู้ดูแลระบบสารสนเทศ

๒ การแจ้งเตือนเมื่อระบบทำงานผิดปกติ เช่น ฮาร์ดดิสก์เต็ม เป็นต้น

๓ การแจ้งเตือนจากโปรแกรมบริหารจัดการเครือข่าย

๔ การแจ้งเตือนจากระบบควบคุมการเข้าถึง

๕ การแจ้งเตือนจากระบบป้องกันการบุกรุก

๖ การแจ้งเตือนการทำงานของระบบเกิดการล้มเหลวหรือหยุดชะงัก

๗๙.๗ กำหนดให้มีการเฝ้าระวังและตรวจสอบการเปลี่ยนแปลงหรือความพยายามในการเปลี่ยนแปลงค่าคอนฟิกกูเรชันด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๗๙.๘ กำหนดให้มีการทบทวนข้อมูลล็อกประเภทต่างๆ ที่กล่าวถึงในหัวข้อนี้อย่างสม่ำเสมอ เช่น ทุกไตรมาส

๑ ระบบงานที่มีความสำคัญ

๒ ระบบงานที่มีข้อมูลสำคัญ

๓ ระบบงานที่เคยถูกบุกรุกหรือใช้ผิดวัตถุประสงค์

๔ ระบบงานที่มีการเชื่อมโยงกับระบบงานอื่นๆ

๗๙.๙ กำหนดให้มีการทบทวนผลของการดำเนินการเชิงแก้ไขนั้น เพื่อให้มั่นใจได้ว่าปัญหาที่พบนั้นได้รับการดำเนินการอย่างเหมาะสม

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๘๐.๑ มีการบันทึกข้อมูลล็อกเกี่ยวกับการทำงานผิดพลาดหรือข้อผิดพลาด (Fault Log)

๘๐.๒ เปิดใช้งานฟังก์ชันสำหรับบันทึกการทำงานผิดพลาดหรือข้อผิดพลาดของระบบเทคโนโลยีสารสนเทศ

๘๐.๓ กำหนดขั้นตอนปฏิบัติสำหรับการจัดการกับการทำงานผิดพลาดหรือข้อผิดพลาดของระบบเทคโนโลยีสารสนเทศ

๘๐.๔ กำหนดให้มีการเฝ้าระวังและตรวจสอบข้อมูลล็อกเกี่ยวกับการทำงานผิดพลาดหรือข้อผิดพลาดของระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๘๐.๕ กำหนดให้มีการวิเคราะห์ข้อมูลล็อกเกี่ยวกับการทำงานผิดพลาดหรือข้อผิดพลาดของระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ และควรดำเนินการเชิงแก้ไขต่อข้อผิดพลาดเหล่านั้นภายในระยะเวลาที่เหมาะสม

๘๐.๖ กำหนดให้มีการทบทวนผลของการดำเนินการเชิงแก้ไขนั้น เพื่อให้มั่นใจได้ว่าข้อผิดพลาดที่พบนั้นได้รับการดำเนินการอย่างเหมาะสมและไม่ทำให้เกิดผลกระทบข้างเคียง ซึ่งรวมถึงมาตรการความมั่นคงปลอดภัยเดิมที่มีอยู่เกิดความเสียหาย

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๘๑.๑ กำหนดมาตรการเพื่อป้องกัน เช่น ควบคุมทางกายภาพไม่ให้เข้าไปแก้ไข Log และควบคุมผู้ที่สามารถล็อกอินเข้าไปแก้ไข Log เป็นต้น

๘๑.๒ กำหนดมาตรการเพื่อป้องกันการเปลี่ยนแปลง แก้ไข หรือลบ Log โดยไม่ได้รับอนุญาต เช่น ใช้การคำนวณผลรวมของ Log (check sum, hash) เป็นต้น

๘๑.๓ กำหนดมาตรการในการเฝ้าระวังและดูแลการทำงานของระบบบันทึก Log อย่างสม่ำเสมอ เพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง

๘๑.๔ กำหนดมาตรการสำหรับการบริหารจัดการเหตุการณ์ต่างๆ ที่เกิดขึ้นกับระบบบันทึก Log เช่น เหตุการณ์ระบบหยุดชะงัก เหตุการณ์ที่ระบบได้บันทึกไว้ใน Log เป็นต้น

๘๑.๕ กำหนดมาตรการเพื่อตรวจสอบพื้นที่บนสื่อบันทึกข้อมูลของระบบบันทึก Log ว่ายังมีพอใช้เพียงพอสำหรับการบันทึก Log หรือไม่ ควรกำหนดให้มีการคำนวณพื้นที่ที่จำเป็นต้องใช้สำหรับการบันทึก Log ว่ามีการใช้วันละเท่าไร และจัดเตรียมสื่อบันทึกข้อมูลให้เพียงพอตามผลของการคำนวณนั้น

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๘๒.๑ ข้อมูลที่ควรบันทึกไว้ ได้แก่ ข้อมูล

๑ กิจกรรมสำคัญที่เกิดขึ้น ซึ่งรวมถึงความสำเร็จ ความล้มเหลว และความผิดพลาด เช่น การเปลี่ยนแปลงหรือแก้ไขต่อไฟล์ที่มีความสำคัญของระบบ เป็นต้น

๒ วัน/เวลาที่เกิดขึ้น

๘๒.๒ มีการเฝ้าระวังและตรวจสอบข้อมูลล็อก ที่เกี่ยวข้องกับกิจกรรมต่างๆ ของผู้ดูแลระบบสารสนเทศอย่างสม่ำเสมอ

๘๒.๓ มีการทบทวนข้อมูลล็อกที่เกี่ยวข้องกับกิจกรรมของผู้ดูแลระบบสารสนเทศอย่างสม่ำเสมอ และควรดำเนินการเชิงแก้ไขต่อปัญหา ที่พบภายในระยะเวลาที่เหมาะสม

นโยบาย

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

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๘๓.๑ มีการตั้งสัญญาณนาฬิกาของระบบเทคโนโลยีสารสนเทศให้ตรงตามเวลามาตรฐานเวลาสากล (Coordinated Universal Time standard) หรือTime Server ของ กฟภ.

๘๓.๒ มีขั้นตอนปฏิบัติเพื่อตรวจสอบและแก้ไขสัญญาณนาฬิกาให้มีความเที่ยงตรงอยู่เสมอ

๘๓.๓ มีการตรวจสอบว่าการประทับตราเวลา (Time Stamp) ของระบบเทคโนโลยีสารสนเทศของ กฟภ. ลงในไฟล์ต่างๆ มีความถูกต้องหรือไม่

๘๓.๔ ระมัดระวังเรื่องรูปแบบของวัน/เวลาที่ระบบเทคโนโลยีสารสนเทศของ กฟภ. ประทับลงในไฟล์และการตีความรูปแบบนั้นให้มีความถูกต้อง เช่น ISO ๘๖๐๑ ใช้ ปี/เดือน/วัน

นโยบาย

๘๔) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรกำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ โดยมีแนวทางตามขั้นตอนปฏิบัติการควบคุมการติดตั้งซอฟต์แวร์ (ภาคผนวก ๖)

นโยบาย

๘๕) ผู้รับผิดชอบสารสนเทศต้องบริหารจัดการช่องโหว่ทางเทคนิค ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๘๕.๑ จัดทำบัญชีรายชื่อของระบบเทคโนโลยีสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น บัญชีรายชื่อฯ ควรมีการบันทึกข้อมูลดังนี้

๑ ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน

๒ สถานที่ที่ติดตั้ง

๓ เครื่องที่ติดตั้ง

๔ ผู้ผลิตซอฟต์แวร์

๕ ข้อมูลสำหรับติดต่อผู้ผลิตซอฟต์แวร์

๖ ผู้รับผิดชอบซอฟต์แวร์นี้ภายใน กฟภ.

๘๕.๒ กำหนดกระบวนการบริหารจัดการช่องโหว่ของระบบเทคโนโลยีสารสนเทศของ กฟภ.

๘๕.๓ กำหนดผู้มีหน้าที่รับผิดชอบในการเฝ้าระวัง ติดตาม และประเมินความเสี่ยงสำหรับช่องโหว่ของระบบเทคโนโลยีสารสนเทศ รวมทั้งประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

๘๕.๔ กระบวนการบริหารจัดการช่องโหว่ควรครอบคลุมประเด็นดังนี้

๑ กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบเทคโนโลยีสารสนเทศของ กฟภ.

๒ กำหนดให้มีการปรับปรุงแหล่งข้อมูลข่าวสารเพื่อให้สอดคล้องกับบัญชีรายชื่อของระบบเทคโนโลยีสารสนเทศของ กฟภ.

๓ กำหนดให้มีการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น รวมทั้งให้ประเมินความเสี่ยงของการติดตั้งโปรแกรมแก้ไขช่องโหว่เมื่อเทียบกับความเสี่ยงของช่องโหว่เอง

๔ กำหนดให้มีการจัดลำดับความสำคัญเพื่อดำเนินการแก้ไขช่องโหว่ที่มีความเสี่ยงสูงก่อนที่มีความเสี่ยงต่ำกว่า

๕ กำหนดให้มีการดำเนินการเชิงแก้ไขโดยเร็วสำหรับช่องโหว่ที่มีระดับความสำคัญสูง หรือหามาตรการที่เหมาะสมเพื่อลดความเสี่ยงที่พบนั้น สำหรับกรณีที่ยังไม่มีโปรแกรมสำหรับแก้ไขช่องโหว่ ควรกำหนดให้

– ทำการปิดบริการหรือปิดฟังก์ชันที่มีช่องโหว่นั้นไว้ชั่วคราว

– ดำเนินการปรับหรือเพิ่มมาตรการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศที่มีช่องโหว่นั้น

– ใช้ไฟร์วอลล์เพื่อควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศที่มีช่องโหว่นั้น
– มีการเฝ้าระวังระบบเทคโนโลยีสารสนเทศที่มีช่องโหว่นั้นอย่างใกล้ชิด
๖ กำหนดให้มีการระบุระยะเวลาที่จะดำเนินการแก้ไขช่องโหว่ เมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น
๗ กำหนดให้มีการทดสอบโปรแกรมแก้ไขช่องโหว่ก่อนที่จะดำเนินการติดตั้งจริงเพื่อป้องกันผลข้างเคียง เช่น ทำให้ระบบงานไม่สามารถให้บริการได้ เป็นต้น
๘ กำหนดให้มีการบันทึกกิจกรรมการดำเนินการต่างๆ ที่ได้ปฏิบัติไปสำหรับช่องโหว่นั้น

๘๕.๕ กำหนดให้มีการเฝ้าระวัง ติดตาม และประเมินระบบเทคโนโลยีสารสนเทศภายหลังจากที่ได้ดำเนินการแก้ไขช่องโหว่ไปแล้ว เพื่อดูว่าระบบทำงานสมบูรณ์และตามปกติหรือไม่

นโยบาย

๘๖) ผู้ดูแลระบบสารสนเทศต้องกำหนดสิทธิ์ให้ผู้ใช้ติดตั้งซอฟแวร์ได้เท่าที่จำเป็น ตามระเบียบคำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้
๘๖.๑ กำหนดสิทธิ์ให้ผู้ใช้ติดตั้งซอฟแวร์ได้เท่าที่จำเป็น และไม่ติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ในเครื่องของ กฟภ.
๘๖.๒ กำหนดรายชื่อซอฟแวร์ที่ติดตั้งได้
๘๖.๓ กำหนดวิธีปฏิบัติในการร้องขอติดตั้งซอฟแวร์

นโยบาย

๘๗) ผู้ตรวจสอบภายในของ กฟภ. ต้องทำแผนและข้อกำหนดการตรวจสอบ รวมถึงกิจกรรมที่เกี่ยวข้องกับการตรวจสอบระบบสารสนเทศ โดยได้รับความเห็นชอบจากผู้รับผิดชอบสารสนเทศเพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของกระบวนการทางธุรกิจ

แนวทางปฏิบัติ

๘๗.๑ ผู้ตรวจสอบภายในของ กฟภ. ควรมีการระบุความต้องการในการตรวจสอบระบบให้บริการ
๘๗.๒ ควรมีการตกลงกันสำหรับขอบเขตการตรวจสอบระหว่างผู้ตรวจสอบภายในของ กฟภ. กับผู้รับตรวจ
๘๗.๓ ผู้รับผิดชอบสารสนเทศควรกำหนดให้ผู้ตรวจสอบภายในของ กฟภ. สามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ในลักษณะที่อ่านได้เพียงอย่างเดียว
๘๗.๔ ในกรณีที่จำเป็นต้องเขียนหรือบันทึกข้อมูลต้องสร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบภายในของ กฟภ. ทำงานบนข้อมูลสำเนา ผู้รับผิดชอบสารสนเทศต้องทำลายหรือลบทิ้งโดยทันทีที่ตรวจสอบเสร็จ

๘๗.๕ ผู้รับผิดชอบสารสนเทศควรมีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึก Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

นโยบาย

๘๘) หน่วยงานผู้รับผิดชอบสารสนเทศต้องป้องกันไม่ให้มีการเข้าถึงข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) โดยไม่ได้รับอนุญาต

แนวทางปฏิบัติ

หน่วยงานผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๘๘.๑ กำหนดให้มีการจัดเก็บข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) ไว้ในสถานที่ที่มีความมั่นคงปลอดภัยเพียงพอ

๘๘.๒ ควบคุมการเข้าถึงข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) โดยจำกัดจำนวนผู้ที่สามารถเข้าถึงได้ตามความจำเป็นในการใช้งาน

นโยบาย

๘๙) คณะกรรมการต้องกำหนดนโยบายและขั้นตอนการปฏิบัติ เพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยน หรือใช้ข้อมูลร่วมกัน ผ่านระบบสารสนเทศที่มีการเชื่อมต่อระหว่างระบบสารสนเทศต่างๆ

หมวด ๙
ความมั่นคงปลอดภัยด้านเครือข่าย

วัตถุประสงค์

เพื่อควบคุมการบริหารจัดการเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอก กฟภ. รวมถึงการควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศกับหน่วยงานภายนอกให้มีความมั่นคงปลอดภัย

นโยบาย

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

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๙๐.๑ กำหนดมาตรการทางเครือข่ายเพื่อป้องกันข้อมูลในเครือข่ายของ กฟภ. จากการถูกเข้าถึงหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต

๙๐.๒ กำหนดมาตรการต่างๆ เพื่อป้องกันระบบงานหรือบริการต่างๆ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต

๙๐.๓ กำหนดให้มีการแยกหน้าที่ความรับผิดชอบในการดูแลเครือข่าย

๙๐.๔ กำหนดมาตรการเพื่อป้องกันระบบเทคโนโลยีสารสนเทศของ กฟภ. ที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ เช่น การใช้ไฟร์วอลล์ เพื่อจำกัดหรือควบคุมการเชื่อมต่อกับเครื่องให้บริการของ กฟภ. เป็นต้น

๙๐.๕ กำหนดมาตรการสำหรับการเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่างๆ เพื่อให้สามารถใช้งานได้อย่างต่อเนื่องมากที่สุด

๙๐.๖ กำหนดให้มีการบันทึก Log ของอุปกรณ์เครือข่ายต่างๆ เพื่อใช้ในการตรวจสอบกิจกรรมต่างๆ ที่เกิดขึ้นอย่างสม่ำเสมอ

นโยบาย

๙๑) ผู้ดูแลระบบสารสนเทศต้องควบคุมให้มีการกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับของการให้บริการ และความต้องการด้านการบริหารจัดการของการให้บริการเครือข่ายทั้งหมดลงในข้อตกลง หรือสัญญาการให้บริการด้านเครือข่ายต่างๆ ทั้งที่เป็นการให้บริการจากภายใน หรือภายนอก

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๙๑.๑ ในข้อตกลงควรกำหนดคุณสมบัติผู้ให้บริการภายนอก เช่น ต้องมีความรู้ความสามารถในการบริหารจัดการเครือข่าย และมีใบรับรองหรือประกาศนียบัตรต่างๆ เป็นต้น

๙๑.๒ ในข้อตกลงควรกำหนดคุณสมบัติทางด้านความมั่นคงปลอดภัยใช้สำหรับการสร้างความมั่นคงปลอดภัยในการให้บริการเครือข่าย ได้แก่ การพิสูจน์ตัวตน การเข้ารหัสข้อมูล การเชื่อมต่อทางเครือข่าย

๙๑.๓ ในข้อตกลงควรกำหนดให้ กฟภ. สามารถดำเนินการตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอกนั้นได้

นโยบาย

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

แนวทางปฏิบัติ

ผู้ดูแลระบบสารสนเทศควรปฏิบัติดังนี้

๙๒.๑ ประเมินความเสี่ยงสำหรับการจัดแบ่งเครือข่ายภายในหน่วยงาน และกำหนดมาตรการป้องกันสำหรับเครือข่ายย่อยที่ได้จัดแบ่ง

๙๒.๒ จัดแบ่งพื้นที่ใช้งานออกเป็นเครือข่ายภายในและเครือข่ายภายนอก

๙๒.๓ แบ่งแยกกลุ่มเครือข่ายที่เหมาะสม โดยแบ่งแยกเป็น เครือข่ายตามกลุ่มของบริการ เครือข่ายตามผู้ใช้ เครือข่ายตามระบบงานต่างๆ ของ กฟภ. ด้วยอุปกรณ์รักษาความมั่นคงปลอดภัยที่เหมาะสม

๙๒.๔ ควบคุมการเข้าถึงทางกายภาพสำหรับเครือข่าย เพื่อป้องกันการเข้าถึงทางกายภาพต่อเครือข่ายย่อยและป้องกันการเปลี่ยนแปลงแก้ไขสายสัญญาณ แอบดักดูข้อมูลบนเครือข่าย

๙๒.๕ กรอง จำกัด และควบคุมการไหลของข้อมูลระหว่างเครือข่ายย่อย

๙๒.๖ แยกเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่นๆ ของ กฟภ. ตามความจำเป็น

๙๒.๗ แบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ โดยใช้อุปกรณ์เฉพาะและควบคุมการไหลของข้อมูลระหว่างเครือข่ายย่อย เหล่านั้น ด้วยวิธีการที่เหมาะสม

๙๒.๘ กรองและจำกัดการไหลของข้อมูลระหว่างเครือข่าย

๙๒.๙ ควบคุมการเข้าถึงเครือข่าย ทั้งจากภายในและภายนอก โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่าย

๙๒.๑๐ แยกวงของเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่นๆ ของหน่วยงาน

๙๒.๑๑ แยกกลุ่มเครือข่ายเป็น ๓ ประเภทใหญ่ๆ คือ (๑) ระบบเครือข่ายภายใน (๒) ระบบเครือข่ายภายนอก และ (๓) ส่วนที่มีการที่เชื่อมต่อทั้งเครือข่ายภายในและเครือข่ายภายนอก

นโยบาย

๙๓) ผู้รับผิดชอบสารสนเทศต้องควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์ โดยมีแนวทางตามขั้นตอนปฏิบัติการจัดระดับชั้นข้อมูลเรื่องการแลกเปลี่ยนสารสนเทศ (ภาคผนวก ๒)

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๙๔.๑ การแลกเปลี่ยนข้อมูลสารสนเทศของ กฟภ. กับหน่วยงานภายนอก ควรได้รับการอนุมัติจาก ผวก. หรือที่ผู้ที่ได้รับมอบอำนาจจาก ผวก. ก่อนทุกครั้ง และมีการควบคุมโดยการระบุข้อตกลงเป็นลายลักษณ์อักษร รวมถึงกำหนดเงื่อนไขสำหรับการแลกเปลี่ยน ตลอดจนมีการป้องกันข้อมูลสารสนเทศตามลำดับชั้นความลับข้อมูลอย่างเหมาะสม

๙๔.๒ การกำหนดข้อตกลงฯ ควรมีการกำหนด ดังนี้

๑ หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง

๒ ผู้ที่เป็นเจ้าของข้อมูลสารสนเทศและสิทธิการใช้ข้อมูลหรือซอฟต์แวร์

๓ ขั้นตอนปฏิบัติสำหรับการแลกเปลี่ยนข้อมูล (เช่น วิธีการส่ง วิธีการรับ เป็นต้น)
๔ ขั้นตอนปฏิบัติสำหรับการตรวจสอบว่าใครเป็นผู้ส่งข้อมูลและใครเป็นผู้รับข้อมูล ทั้งนี้เพื่อเป็นการป้องกันการปฏิเสธ
๕ ขั้นตอนปฏิบัติสำหรับการป้องกันข้อมูล
๖ การจัดทำหีบห่อเพื่อให้การจัดส่งข้อมูลมีความมั่นคงปลอดภัย
๗ การจัดทำป้ายบ่งชี้เพื่อระบุว่าเป็นข้อมูลหรือเอกสารสำคัญ
๘ วิธีการในการจัดส่งเอกสาร
๙ ความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่นๆ กับข้อมูลนั้น
๑๐ ปฏิบัติตามเงื่อนไขต่างๆ ที่จะต้องปฏิบัติตาม เช่น กฎหมายลิขสิทธิ์ ใบอนุญาตการใช้งานซอฟต์แวร์ (Software license) เป็นต้น

นโยบาย

๙๕) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic messaging) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศและผู้ใช้ควรปฏิบัติดังนี้
๙๕.๑ ในการส่งข้อมูลที่เป็นความลับ เช่น ข้อมูลเงินเดือน ต้องเข้ารหัสข้อมูล และห้ามส่งรหัสผ่านไปกับข้อมูล เป็นต้น
๙๕.๒ ไม่เขียน หรือพิมพ์ข้อความที่ไม่เหมาะสม หรือไม่ทำการใดๆ ที่มีความเสี่ยงต่อการละเมิด พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

นโยบาย

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

นโยบาย

๙๗) หน่วยงานที่มีการจัดหาหรือจัดให้มีการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ต้องระบุความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบงานที่พัฒนาขึ้นมาใช้งาน นับตั้งแต่เริ่มต้นออกแบบระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

หน่วยงานที่มีการจัดหาหรือจัดให้มีการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิมควรปฏิบัติดังนี้

๙๗.๑ ประเมินความเสี่ยงสำหรับระบบงานที่จะจัดหาหรือพัฒนาขึ้นมาใช้งาน และระบุข้อกำหนดด้านความมั่นคงปลอดภัยที่ต้องมีหรือปฏิบัติเพื่อลดความเสี่ยงที่ได้ประเมิน

๙๗.๒ ระบุข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบงานที่จะจัดหาหรือพัฒนาขึ้นมาใช้งาน นับตั้งแต่เริ่มต้นออกแบบระบบ

๙๗.๓ ระบุข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับซอฟต์แวร์ที่จะจัดซื้อหรือจัดหามาใช้งาน

๙๗.๔ พิจารณาความสำคัญของข้อมูล ในระบบงานที่จะพัฒนาหรือจัดหามาใช้งาน และระบุข้อกำหนดด้านความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันข้อมูลนั้น

๙๗.๕ ทดสอบเพื่อประเมินซอฟต์แวร์หรือระบบงานที่จัดหามาใช้งานว่าตรงตามข้อกำหนดด้านความมั่นคงปลอดภัยที่ระบุไว้หรือไม่

๙๗.๖ ทำสัญญา และระบุข้อกำหนดด้านความมั่นคงปลอดภัยให้ผู้พัฒนาหรือผู้จัดหาภายนอกปฏิบัติตาม

๙๗.๗ พิจารณาปิดการใช้งานฟังก์ชันเพิ่มเติมหรือที่ไม่มีความจำเป็นต่อการใช้งานของซอฟต์แวร์ที่จัดซื้อหรือจัดหามาใช้งาน ทั้งนี้เพื่อลดความเสี่ยงอันเนื่องมาจากฟังก์ชันดังกล่าว

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๙๘.๑ กำหนดมาตรการการพิสูจน์ตัวตนสำหรับผู้เข้าใช้ระบบงานพาณิชย์อิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัยเพียงพอ

๙๘.๒ กำหนดมาตรการป้องกันข้อมูลลับ ข้อมูลสำคัญ หรือข้อมูลส่วนบุคคลในระบบงานพาณิชย์อิเล็กทรอนิกส์

๙๘.๓ กำหนดวิธีการตรวจสอบข้อมูลการชำระเงินของลูกค้า กล่าวคือ กฟภ.จะสามารถตรวจสอบได้ว่าลูกค้าได้ชำระเงินแล้วหรือไม่ หรือในทางกลับกัน ลูกค้าสามารถตรวจสอบได้ว่า กฟภ. ได้รับเงินค่าสินค้าแล้วหรือไม่

๙๘.๔ กำหนดให้มีการระบุถึงความรับผิดชอบของ กฟภ. กรณีที่มีการฉ้อโกงเกิดขึ้นกับธุรกรรมทางอิเล็กทรอนิกส์ของลูกค้า

๙๘.๕ กำหนดมาตรการการป้องกันข้อมูล เช่น การเข้ารหัสข้อมูล เพื่อป้องกันกิจกรรมการทำธุรกรรมทางอิเล็กทรอนิกส์ของลูกค้า เป็นต้น

นโยบาย

๙๙) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องป้องกันไม่ให้มีการแก้ไขเปลี่ยนแปลงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาตและรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ ที่มีการเผยแพร่ต่อสาธารณชน ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๙๙.๑ กำหนดให้มีการป้องกันข้อมูลหรือซอฟต์แวร์ที่สำคัญที่ปรากฏในระบบงานสาธารณะ เช่น บนเว็บไซต์จากการถูกเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต เป็นต้น

๙๙.๒ กำหนดให้มีการประเมินความเสี่ยงต่อระบบงานสาธารณะและข้อมูลสำคัญในระบบ และกำหนดมาตรการลดความเสี่ยงก่อนที่จะเริ่มเปิดให้บริการระบบดังกล่าว

๙๙.๓ กำหนดให้มีกระบวนการตรวจสอบความถูกต้องและเหมาะสม และอนุมัติข้อมูลก่อนที่จะทำการเผยแพร่ข้อมูลนั้นในระบบงานสาธารณะ

๙๙.๔ กำหนดมาตรการป้องกันเพื่อไม่ให้ผู้ที่สามารถใช้งานระบบงานสาธารณะสามารถใช้ระบบนี้เป็นทางผ่านไปสู่เครือข่ายอื่นๆ ที่เชื่อมต่อกับระบบงานนี้

นโยบาย

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

แนวทางปฏิบัติ

หน่วยงานที่เกี่ยวข้องในการทำธุรกรรมทางออนไลน์ควรปฏิบัติดังนี้

๑๐๐.๑ กำหนดให้มีการใช้ลายมือชื่ออิเล็กทรอนิกส์ เพื่อป้องกันธุรกรรมทางอิเล็กทรอนิกส์ที่มีความสำคัญ เช่น ป้องกันจากการถูกสวมรอยทำธุรกรรมแทนเจ้าตัว เป็นต้น

๑๐๐.๒ กำหนดให้มีกระบวนการบริหารจัดการการใช้ลายมือชื่ออิเล็กทรอนิกส์ การออกหรือการใช้ใบรับรองอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย

๑๐๐.๓ กำหนดมาตรการการพิสูจน์ตัวตนสำหรับผู้เข้าทำธุรกรรมทางอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัยเพียงพอ

๑๐๐.๔ กำหนดให้มีการเข้ารหัสข้อมูลและ/หรือใช้โพรโตคอลที่มีความมั่นคงปลอดภัยสำหรับข้อมูลที่จะมีการส่งผ่านเครือข่ายหรือระบบสื่อสารระหว่างลูกค้ากับระบบงานให้บริการธุรกรรมทางอิเล็กทรอนิกส์

๑๐๐.๕ กำหนดให้มีการจัดเก็บข้อมูลธุรกรรมทางอิเล็กทรอนิกส์ไว้บนสื่อบันทึกข้อมูลที่ไม่สามารถเข้าถึงได้โดยผู้อื่น รวมทั้งควรจัดเก็บไว้เพื่อไม่ให้สามารถเข้าถึงได้โดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เป็นต้น

นโยบาย

๑๐๑) ผู้พัฒนาระบบสารสนเทศต้องพัฒนาซอฟต์แวร์และระบบสารสนเทศอย่างมั่นคงปลอดภัยตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรปฏิบัติดังนี้

๑๐๑.๑ สภาพแวดล้อมในการพัฒนาฯ ควรมีความมั่นคงปลอดภัย เช่น สถานที่ ระบบคอมพิวเตอร์ ระบบเครือข่าย ฐานข้อมูล ซอฟต์แวร์ เป็นต้น

๑๐๑.๒ เขียนโปรแกรมแต่ละภาษา ให้ปลอดภัย (secure coding)

๑๐๑.๓ มีจุดตรวจความมั่นคงปลอดภัยในแต่ละขั้นตอนหลักในโครงการพัฒนาระบบสารสนเทศ

๑๐๑.๔ ที่เก็บข้อมูลและส่วนประกอบของการพัฒนาซอฟต์แวร์ควรมีความปลอดภัย

๑๐๑.๕ มีความมั่นคงปลอดภัยสำหรับระบบที่จัดเก็บการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์หนึ่งหรือหลายไฟล์ (version control) เช่น ให้ผู้มีสิทธิเท่านั้น จัดเก็บไว้ในที่ปลอดภัย เป็นต้น

๑๐๑.๖ ปิดช่องโหว่ และควบคุมไม่ให้ช่องโหว่นั้นกลายเป็นจุดอ่อนของระบบ

นโยบาย

๑๐๒) ผู้พัฒนาระบบสารสนเทศต้องมีขั้นตอนการควบคุมการเปลี่ยนแปลงระบบสารสนเทศเป็นลายลักษณ์อักษร เพื่อควบคุมให้ระบบเป็นไปตามข้อตกลงที่กำหนดไว้และมีความมั่นคงปลอดภัยตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรปฏิบัติดังนี้

๑๐๒.๑ กำหนดขั้นตอนการควบคุมการเปลี่ยนแปลงระบบสารสนเทศเป็นลายลักษณ์อักษร (การเปลี่ยนแปลงดังกล่าวครอบคลุมถึง การขอให้พัฒนาหรือปรับปรุงระบบงานเพิ่มเติมตามคำขอ การเปลี่ยนแปลงฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น)

๑๐๒.๒ ขั้นตอนปฏิบัติฯ ควรครอบคลุมประเด็นดังนี้

๑ กำหนดผู้ทำหน้าที่ขออนุมัติการเปลี่ยนแปลง และผู้มีอำนาจอนุมัติการเปลี่ยนแปลงนั้น

๒ กำหนดให้มีการชี้แจงเหตุผลของการขอเปลี่ยนแปลงนั้น

๓ กำหนดให้มีการพิจารณาผลกระทบและความเร่งด่วนในการดำเนินการ

๔ กำหนดให้มีการระบุรายละเอียดของสิ่งที่จะดำเนินการเปลี่ยนแปลง เช่น การเปลี่ยนแปลงต่อ ซอฟต์แวร์ ฮาร์ดแวร์ ฐานข้อมูล เป็นต้น

๕ กำหนดให้มีการวางแผนและดำเนินการทดสอบตามความจำเป็น

๖ กำหนดให้มีการติดตั้งจริงภายหลังการทดสอบเสร็จ

๗ กำหนดให้มีการรายงานผลภายหลังการติดตั้ง

๑๐๒.๓ ในการขออนุมัติการเปลี่ยนแปลงระบบงาน กฟภ. ควรกำหนดให้ผู้ที่เกี่ยวข้องปฏิบัติดังนี้

๑ พิจารณาความเสี่ยงที่มีต่อระบบงาน (สำหรับการเปลี่ยนแปลงที่จะดำเนินการนั้น) และกำหนดมาตรการลดความเสี่ยงที่จำเป็นก่อนที่จะดำเนินการเปลี่ยนแปลง

๒ พิจารณาผลกระทบที่มีต่อระบบงาน เช่น การเปลี่ยนแปลงนั้นอาจส่งผลให้เกิดการหยุดชะงักต่อกระบวนการทางธุรกิจสำคัญ เป็นต้น

๓ กำหนดมาตรการป้องกันที่จำเป็นเพื่อรองรับต่อการเปลี่ยนแปลงดังกล่าว

๔ ระมัดระวังเพื่อไม่ให้การเปลี่ยนแปลงที่จะดำเนินการนั้นไปทำให้มาตรการหรือขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยที่มีอยู่แล้วเดิมเกิดความเสียหายหรือทำให้เกิดการละเมิดความมั่นคงปลอดภัยได้

๕ ควบคุมการเข้าถึงของผู้พัฒนาระบบสารสนเทศโดยกำหนดให้สามารถเข้าถึงได้เฉพาะในส่วนของเครื่องสำหรับทำการพัฒนาระบบ ระบบงาน ไลบรารี่ หรือไดเร็คทอรี่ที่จำเป็นต่อการปฏิบัติงานของผู้พัฒนาระบบสารสนเทศนั้นเท่านั้น

๖ ทดสอบระบบงานโดยผู้ใช้อย่างครอบคลุมและกำหนดให้ผู้ใช้ลงนามรับรองการใช้งาน

๗ ดำเนินการปรับปรุงเอกสารต่างๆ ที่เกี่ยวข้องกับระบบงานให้มีความทันสมัย เช่น เอกสารคู่มือการใช้งาน เอกสารวิเคราะห์และออกแบบระบบ เป็นต้น รวมทั้งจัดเก็บหรือทำลายเอกสารเดิมตามความจำเป็น เช่น เอกสารสำหรับระบบงานเวอร์ชั่นเก่า

๘ บันทึกข้อมูลที่เกี่ยวข้องกับการขออนุมัติการเปลี่ยนแปลงนั้นไว้ เพื่อเอาไว้ใช้ในการเรียนรู้ในภายหลังหรือ เป็นหลักฐานในการตรวจสอบในภายหลังได้

นโยบาย

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

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรปฏิบัติดังนี้

๑๐๓.๑ กรณีมีการเปลี่ยนแปลงต่อระบบปฏิบัติการคอมพิวเตอร์ของระบบสารสนเทศ (ซึ่งรวมถึงการติดตั้งระบบปฏิบัติการเวอร์ชันใหม่ และการติดตั้งโปรแกรมแก้ไขช่องโหว่ของระบบปฏิบัติการ) กฟภ. ควรกำหนดให้มีการวางแผนเพื่อดำเนินการเปลี่ยนแปลงนั้น รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในการดำเนินการ

๑๐๓.๒ กำหนดให้มีการแจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการดำเนินการเปลี่ยนแปลงระบบปฏิบัติการนั้น

๑๐๓.๓ กำหนดให้มีการทดสอบระบบงานที่จะมีการเปลี่ยนแปลงระบบปฏิบัติการให้ครอบคลุม ก่อนที่จะดำเนินการเปลี่ยนแปลงนั้น

๑๐๓.๔ กำหนดให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่ได้เปลี่ยนแปลงระบบปฏิบัติการไปแล้ว เพื่อติดตามความสมบูรณ์ของการทำงาน และดูว่ามีผลกระทบต่อมาตรการความมั่นคงปลอดภัยของระบบงานนั้นหรือไม่

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๐๔.๑ ในกรณีที่จำเป็นต้องปรับปรุงหรือเปลี่ยนแปลงต่อซอฟต์แวร์สำเร็จรูปที่ใช้งาน (Software package) ควรปฏิบัติดังนี้

๑ ตรวจสอบเงื่อนไขหรือข้อตกลงการใช้งานก่อนว่าจำเป็นต้องได้รับการอนุมัติจากผู้ผลิตซอฟต์แวร์ก่อนดำเนินการเปลี่ยนแปลงใดๆ หรือไม่ ทั้งนี้เพื่อป้องกันการละเมิดลิขสิทธิ์

๒ พิจารณาหรือตรวจสอบว่าการเปลี่ยนแปลงนั้นจะก่อให้เกิดความเสียหายต่อมาตรการความมั่นคงปลอดภัยของซอฟต์แวร์นั้นหรือไม่

๑๐๔.๒ กำหนดให้มีการประสานงานกับ เจ้าของลิขสิทธิ์ในซอฟต์แวร์เพื่อให้การเปลี่ยนแปลงที่ได้ดำเนินไปนั้นได้รับการตอบรับเพื่อบรรจุไว้เป็นส่วนหนึ่งของ ซอฟต์แวร์สำเร็จรูปที่ใช้งาน (Software package) นั้น เช่น ในเวอร์ชันถัดไป รวมทั้งกำหนดให้มีการพิจารณาผลกระทบที่ กฟภ. อาจต้องรับผิดชอบต่อการบำรุงรักษาซอฟต์แวร์นั้นด้วยตนเองต่อไปในอนาคต กล่าวคือ สำหรับกรณีที่ เจ้าของลิขสิทธิ์ในซอฟต์แวร์ ไม่บรรจุเข้าไว้เป็นส่วนหนึ่งของซอฟต์แวร์สำเร็จรูปที่ใช้งาน (Software package) นั้น

๑๐๔.๓ กำหนดให้มีการปรับปรุงหรือเปลี่ยนแปลงต่อซอฟต์แวร์แพคเก็จที่เป็นฉบับสำเนาและเก็บตัวต้นฉบับไว้ในสภาพเดิม

๑๐๔.๔ กำหนดให้มีการทดสอบซอฟต์แวร์แพคเก็จที่ได้ทำการปรับปรุงหรือแก้ไขเองนั้นให้ครอบคลุมก่อนที่จะดำเนินการติดตั้ง

๑๐๔.๕ กำหนดให้มีการบันทึกลายลักษณ์อักษรเกี่ยวกับรายละเอียดของการปรับปรุงหรือเปลี่ยนแปลงต่อซอฟต์แวร์แพคเก็จนั้น เพื่อในกรณีที่จำเป็นต้องดำเนินการเพิ่มเติมอีกในอนาคต จะได้ทราบรายละเอียดการดำเนินการที่ได้ทำไปแล้ว

๑๐๔.๖ กำหนดให้มีหน่วยงานภายนอกอิสระหรือผู้ที่มีความรู้ความสามารถในการประเมินซอฟต์แวร์ทำหน้าที่ในการประเมินซอฟต์แวร์แพคเก็จที่ กฟภ. ได้ทำการปรับปรุงเองนั้น

นโยบาย

๑๐๕) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องพัฒนาและติดตั้งใช้งานระบบสารสนเทศโดยคำนึงถึงหลักการความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๐๕.๑ ให้สิทธ์ต่ำที่สุด (Lest Privilege) แก่ผู้ใช้ เพื่อป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต

๑๐๕.๒ ให้สิทธ์เฉพาะที่จำเป็นในการปฏิบัติงาน (Need to Know) แก่ผู้ใช้เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ

๑๐๕.๓ พัฒนาระบบสารสนเทศในลักษะเปิด (Open Design) เพื่อให้การพัฒนาระบบสารสนเทศมี อัลกอริทึม (Algorithm) ที่เป็นมาตรฐานเดียวกัน และสามารถตรวจสอบการทำงานได้

นโยบาย

๑๐๖) ผู้พัฒนาระบบสารสนเทศต้องกำหนดมาตรการป้องกันสภาพแวดล้อมการพัฒนาระบบอย่างมั่นคงปลอดภัยให้ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรกำหนดมาตรการป้องกันสภาพแวดล้อมการพัฒนาระบบอย่างมั่นคงปลอดภัยให้ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ โดยต้องป้องกันข้อมูลของระบบที่เกิดขึ้นในระหว่างการพัฒนา การับส่งข้อมูล การสำรองข้อมูล และการควบคุมการเข้าถึงระบบสารสนเทศ

นโยบาย

๑๐๗) เจ้าของระบบสารสนเทศต้องดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างพัฒนาซอฟต์แวร์ ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

เจ้าของระบบสารสนเทศควรปฏิบัติดังนี้

๑๐๗.๑ กำหนดให้มีการจัดทำสัญญาจ้างการพัฒนาระบบงานโดยให้ครอบคลุมทั้งด้านคุณภาพและความมั่นคงปลอดภัยของระบบงานที่จะมีการพัฒนาขึ้นมาโดยผู้ให้บริการภายนอก

๑๐๗.๒ กำหนดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก เช่น โดยการบริหารจัดการโครงการตั้งแต่เริ่มต้นจนกระทั่งแล้วเสร็จ

๑๐๗.๓ กำหนดให้มีการระบุว่าใครจะเป็นผู้มีสิทธิหรือเจ้าของในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดของระบบงานภายใต้โครงการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก

๑๐๗.๔ กำหนดให้มีการจัดหาซอฟต์แวร์ที่จะต้องมีการใช้งานภายใต้โครงการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก โดยให้มีจำนวนใบอนุญาตการใช้งานซอฟต์แวร์เหล่านั้นให้ถูกต้องและครบถ้วน

๑๐๗.๕ กำหนดให้มีหน่วยงานภายนอกอิสระหรือผู้ที่มีความรู้ความสามารถในการประเมินซอฟต์แวร์ทำหน้าที่ในการรับรองด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่พัฒนาโดยผู้ให้บริการภายนอกนั้น

๑๐๗.๘ ตรวจสอบโปรแกรมไม่พึงประสงค์ในซอฟต์แวร์

นโยบาย

๑๐๘) ผู้พัฒนาระบบสารสนเทศต้องทดสอบด้านความมั่นคงปลอดภัยของระบบที่พัฒนาใหม่หรือระบบงานเดิมที่ปรับปรุง เพื่อให้แน่ใจว่าระบบสารสนเทศสามารถทำงานได้อย่างมั่นคงปลอดภัยตามความต้องการที่กำหนดไว้ โดยให้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรส่งระบบที่พัฒนาใหม่หรือระบบงานเดิมที่ปรับปรุงให้หน่วยงานที่เกี่ยวข้องทดสอบด้านความมั่นคงปลอดภัย

นโยบาย

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

แนวทางปฏิบัติ

หน่วยงานที่เกี่ยวข้องกับการตรวจรับระบบใหม่ หรือที่ปรับปรุงเพิ่มเติมควรปฏิบัติดังนี้

๑๐๙.๑ กำหนดเกณฑ์ในการตรวจรับระบบใหม่ หรือที่ปรับปรุงเพิ่มเติม ทั้งที่มาจากการพัฒนาภายในองค์กร หรือที่มีการจัดหาจากจ้างพัฒนา อย่างเป็นลายลักษณ์อักษร

๑๐๙.๒ เกณฑ์การตรวจรับควรมีรายละเอียดดังนี้

๑ มีการทดสอบหรือตรวจสอบมาตรการความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศนั้น

๒ มีการจัดทำและส่งมอบคู่มือที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศนั้น

๓ มีการอบรมบุคลากรที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศนั้น

๔ มีการพัฒนาระบบเทคโนโลยีสารสนเทศโดยคำนึงถึงความยากง่ายในการใช้งาน (User friendliness)

๕ มีการพัฒนาระบบเทคโนโลยีสารสนเทศโดยคำนึงถึงการป้องกันความผิดพลาดโดยมนุษย์ในการใช้งานระบบ (Human errors)

๖ มีการระบุข้อกำหนดด้านความต้องการในการกู้คืนระบบเทคโนโลยีสารสนเทศนั้น

๑๐๙.๓ ทดสอบระบบก่อนที่จะนำระบบดังกล่าวมาใช้งานจริง

นโยบาย

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

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรปฏิบัติดังนี้

๑๑๐.๑ ไม่อนุญาตการใช้ข้อมูลส่วนบุคคลหรือข้อมูลสำคัญเพื่อใช้ในการทดสอบกับระบบงาน

๑๑๐.๒ กำหนดให้มีการลบข้อมูลส่วนที่บ่งชี้ตัวบุคคลทิ้งไปก่อนนำข้อมูลนั้นไปใช้ในการทดสอบกับระบบงาน เช่น ลบชื่อนามสกุลทิ้งไป เป็นต้น

๑๑๐.๓ กำหนดให้มีการลบข้อมูลส่วนที่มีความสำคัญทิ้งไปก่อนนำข้อมูลนั้นไปใช้ในการทดสอบกับระบบงาน เช่น ข้อมูลเงินเดือน เป็นต้น

๑๑๐.๔ กำหนดให้มีการขออนุมัติก่อนทุกครั้งก่อนที่จะนำข้อมูลบนเครื่องให้บริการไปใช้ในการทดสอบกับระบบงาน

๑๑๐.๕ กำหนดให้ทำการลบข้อมูลจริงซึ่งนำไปใช้ในการทดสอบโดยทันทีหลังจากที่ใช้งานเสร็จ

นโยบาย

๑๑๑) ผู้พัฒนาระบบสารสนเทศต้องตรวจสอบ (Validate) ข้อมูลใดๆ ก่อนที่จะรับเข้าสู่แอพพลิเคชันเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรปฏิบัติดังนี้

๑๑๑.๑ กำหนดให้มีการตรวจสอบข้อมูลนำเข้าสู่ระบบงาน (แอพพลิเคชั่น) เพื่อให้ข้อมูลนั้นมีความถูกต้องและเหมาะสมก่อนนำไปใช้ในการประมวลผล

๑๑๑.๒ กำหนดให้มีการตรวจสอบข้อมูลนำเข้าระบบงาน (แอพพลิเคชั่น) ดังนี้

๑ ข้อมูลนำเข้าควรตรงกับชนิดของข้อมูลที่ต้องการ

๒ ข้อมูลนำเข้าควรอยู่ภายในช่วงของค่าที่ต้องการ

๓ ข้อมูลนำเข้าควรอยู่ภายในค่าขอบเขตบนและล่างที่ต้องการ

๔ ข้อมูลนำเข้าควรมีความครบถ้วน

๕ ข้อมูลนำเข้าไม่ควรมีตัวอักษรหรืออักขระพิเศษต่างๆ ที่นอกเหนือจากที่ต้องการ

๖ ระบบงาน (แอพพลิเคชั่น) ต้องระบุว่าข้อมูลที่นำเข้าไม่ได้ error เพราะอะไร)

๑๑๑.๓ กำหนดให้มีการตรวจสอบฟิลด์ หรือไฟล์ข้อมูลที่สำคัญๆ อย่างสม่ำเสมอเพื่อตรวจสอบความถูกต้องและเหมาะสมของข้อมูลเหล่านั้น

๑๑๑.๔ กำหนดให้มีการตรวจสอบจากเอกสารที่จะใช้เป็นข้อมูลนำเข้า เพื่อตรวจหาการเปลี่ยนแปลงที่เกิดขึ้นโดยไม่ได้รับอนุญาต เช่น มีการขีดฆ่าหรือลบโดยไม่มีลายมือชื่อกำกับ เป็นต้น

๑๑๑.๕ กำหนดขั้นตอนปฏิบัติสำหรับการจัดการกับข้อผิดพลาดที่ตรวจพบในข้อมูลนำเข้า

๑๑๑.๖ กำหนดบุคลากรที่ทำหน้าที่ในการนำข้อมูลเข้าระบบงาน รวมทั้งกำหนดบทบาทและหน้าที่ความรับผิดชอบ

๑๑๑.๗ กำหนดให้มีการบันทึกล็อกสำหรับกิจกรรมการนำข้อมูลเข้าระบบงาน

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๑๒.๑ ออกแบบระบบงาน (แอพพลิเคชั่น) เพื่อช่วยลดความเสี่ยงในการประมวลผลผิดพลาด เช่น การออกแบบหน้าจอสำหรับรับข้อมูลนำเข้าที่เหมาะสม สามารถช่วยลดความผิดพลาดในการประมวลผลข้อมูลได้ เป็นต้น

๑๑๒.๒ กำหนดขั้นตอนปฏิบัติเพื่อป้องกันระบบงาน (แอพพลิเคชั่น) ทำงานต่อไปหลังจากที่เกิดข้อผิดพลาดขึ้น

๑๑๒.๓ กำหนดขั้นตอนปฏิบัติเพื่อป้องกันระบบงานทำงานผิดลำดับหลังจากที่เกิดข้อผิดพลาดขึ้น

๑๑๒.๔ กำหนดให้มีการออกแบบระบบงานเพื่อป้องกันปัญหาหน่วยความจำล้น (buffer overflows) เช่น การนับจำนวนตัวอักษรหรืออักขระที่รับเข้ามาเพื่อไม่ให้เกินจำนวนตามที่ต้องการ เป็นต้น

๑๑๒.๕ กำหนดให้มีมาตรการเพื่อแก้ไขและกู้กลับคืนไปสู่จุดที่มีการประมวลผลผิดพลาดหรือที่ฐานข้อมูลของระบบงานเกิดความเสียหาย (เช่น ฮาร์ดดิสก์เกิดความเสียหาย) เพื่อให้ระบบงานสามารถประมวลผลต่อไปได้อย่างต่อเนื่องและถูกต้อง

๑๑๒.๖ กำหนดให้มีการตรวจหาข้อผิดพลาดที่เกิดขึ้นจากการประมวลผล เช่น

๑ การตรวจสอบความถูกต้องของผลการประมวลผลแบบกลุ่ม (batch processing) เช่น ด้วยการตรวจนับด้วยมือเมื่อเทียบกับผลการประมวลผลด้วยระบบงาน
๒ การตรวจสอบยอดที่ยกมาโดยเทียบกับยอดที่ปิดไปก่อนหน้านี้ (โดยปกติในทางบัญชียอดที่ยกมาควรเท่ากับยอดที่ปิดไปก่อนหน้านี้)
๓ การคำนวณค่าผลรวมเพื่อดูว่ามีบางรายการเกิดการสูญหายหรือไม่ครบถ้วนหรือไม่ เช่น คำนวณด้วยตนเองในฟิลด์หมายเลขเช็คโดยนำหมายเลขเช็คบวกเข้าด้วยกันทั้งหมด ซึ่งจะได้ค่าผลรวมออกมาเป็นค่าค่าหนึ่ง และนำค่านี้ไปเปรียบเทียบกับค่าผลรวมที่คำนวณด้วยระบบงานสำหรับฟิลด์เดียวกัน
๔ การตรวจสอบข้อมูลล็อกซึ่งแสดงถึงกิจกรรมการประมวลผลที่เกิดขึ้น
๕ การทำงานของระบบงานว่าตรงตามกำหนดการที่วางไว้หรือไม่
๖ การตรวจสอบลำดับการประมวลผลของระบบงานว่าทำงานตามลำดับที่ต้องการหรือไม่
๗ การตรวจสอบว่ามีการสิ้นสุดการทำงานของระบบงานอย่างกะทันหันเกิดขึ้นหรือไม่ (ซึ่งอาจแสดงถึงการทำงานที่ผิดพลาดของระบบงาน)

นโยบาย

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

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรปฏิบัติดังนี้
๑๑๓.๑ ตรวจสอบว่า ผู้ส่งข้อมูลมาคือใคร ถ้าตรวจสอบแล้วว่าเป็นผู้ส่งข้อมูลที่ถูกต้อง ก็จะมีความถูกต้องแท้จริง (Authenticity)
๑๑๓.๒ ตรวจสอบ ข้อมูลที่ส่งมา ว่ามีความถูกต้องครบถ้วน (Integrity) เช่นเดียวกับข้อมูลจากต้นทางหรือไม่

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๑๔.๑ ตรวจสอบข้อมูลที่นำออกจากระบบงาน (แอพพลิเคชั่น) เพื่อตรวจดูความถูกต้อง ความเหมาะสม ความสมบูรณ์ และความสมเหตุสมผล ก่อนนำไปใช้งานหรือใช้ประโยชน์ต่อไป

๑๑๔.๒ กำหนดให้มีผู้รับผิดชอบสำหรับการตรวจสอบข้อมูลที่นำออกจากระบบงาน

๑๑๔.๓ กำหนดให้มีการตรวจสอบข้อมูลนำเข้าระบบงาน (ข้อมูลนั้นนำมาจากอีกระบบงานหนึ่ง) เพื่อให้ข้อมูลมีความถูกต้อง เหมาะสม และสมบูรณ์ ก่อนที่จะนำข้อมูลนั้นเข้าสู่กระบวนการประมวลผลต่อไป

๑๑๔.๔ จัดทำขั้นตอนปฏิบัติเพื่อจัดการกับข้อผิดพลาดที่พบในข้อมูลที่นำออกจากระบบงาน

๑๑๔.๕ กำหนดให้มีการนับจำนวนรายการข้อมูลในระบบงานนั้นเทียบกับรายการข้อมูลที่นำเข้าไปประมวลผลว่าตรงกันหรือไม่ เช่น ขนาดข้อมูล จำนวนฟิล จำนวนrecord

๑๑๔.๖ กำหนดให้มีการบันทึกข้อมูลล็อกแสดงกิจกรรมการตรวจสอบข้อมูลที่นำออกจากระบบงาน

นโยบาย

๑๑๕) ผู้รับผิดชอบสารสนเทศต้องป้องกันการรั่วไหลของข้อมูลสารสนเทศ โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๑๕.๑ ป้องกันโปรแกรมไม่พึงประสงค์ประเภทม้าโทรจัน (Trojan horses) ซึ่งเมื่อถูกติดตั้งลงไปในระบบเทคโนโลยีสารสนเทศของ กฟภ. แล้ว อาจแอบขโมยและส่งข้อมูลขอ กฟภ. ไปให้แก่ผู้ไม่ประสงค์ดีได้

๑๑๕.๒ ตรวจสอบสื่อบันทึกข้อมูลและระบบสื่อสารข้อมูลอย่างสม่ำเสมอเพื่อป้องกันการแอบส่งข้อมูลผ่านทางสื่อบันทึกข้อมูลหรือระบบสื่อสารข้อมูลนั้น

๑๑๕.๓ เข้ารหัสข้อมูลเพื่อซ่อนข้อมูลที่มีการรับส่ง

๑๑๕.๔ ใช้ซอฟต์แวร์หรือระบบงานที่ได้รับการตรวจสอบแล้วว่ามีการทำงานที่ถูกต้องและเชื่อถือได้ หรือใช้ซอฟต์แวร์ที่ได้รับการประเมินและรับรองแล้ว เช่น ตามมาตรฐาน ISO/IEC 15408 Evaluation Criteria for IT Security เป็นต้น

๑๑๕.๕ เฝ้าระวังและตรวจสอบกิจกรรมของผู้ใช้ในระบบงานอย่างสม่ำเสมอ แต่ต้องระมัดระวังไม่ให้ขัดแย้งกับกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการละเมิดสิทธิส่วนบุคคล เป็นต้น

๑๑๕.๖ เฝ้าระวังและตรวจสอบการใช้ทรัพยากรสารสนเทศของ กฟภ.อย่างสม่ำเสมอเพื่อป้องกันการใช้ผิดวัตถุประสงค์

หมวด ๑๑
การจัดการความสัมพันธ์กับผู้ให้บริการภายนอก

วัตถุประสงค์

เพื่อป้องกัน ควบคุม ติดตาม และตรวจสอบ การปฏิบัติงานของหน่วยงานผู้ให้บริการภายนอก ให้มีประสิทธิภาพและมีความมั่นคงปลอดภัยสารสนเทศ

นโยบาย

๑๑๖) ผู้รับผิดชอบสารสนเทศต้องแจ้งให้ผู้ให้บริการภายนอกปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรแจ้งให้ผู้ให้บริการภายนอกปฏิบัติตามระเบียบการไฟฟ้าส่วนภูมิภาคว่าด้วยการจัดการและความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๐ ประกาศนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ พ.ศ. ๒๕๖๑ และแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ ประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ ซึ่งใช้บังคับอยู่ในปัจจุบัน รวมถึงที่จะได้แก้ไขในอนาคต รวมทั้งต้องปฏิบัติตามแนวทางปฏิบัติ หลักเกณฑ์ ประกาศ ระเบียบ กฎหมาย ที่จะมีการประกาศใช้ในอนาคตด้วย

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรระบุข้อตกลงเพื่ออนุญาตให้ผู้ให้บริการภายนอกเข้าถึงระบบสารสนเทศ โดยให้ผู้ให้บริการภายนอกลงนามในหนังสือสัญญาการรักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement) และการปฏิบัติตามระเบียบการไฟฟ้าส่วนภูมิภาคว่าด้วยการจัดการและความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๐ ประกาศนโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ พ.ศ. ๒๕๖๑ และแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ ประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๑ ซึ่งใช้บังคับอยู่ในปัจจุบัน รวมถึงที่จะได้แก้ไขในอนาคต รวมทั้งต้องปฏิบัติตามแนวทางปฏิบัติ หลักเกณฑ์ ประกาศ ระเบียบ กฎหมาย ที่จะมีการประกาศใช้ในอนาคตด้วย

นโยบาย

๑๑๘) ผู้รับผิดชอบสารสนเทศต้องควบคุมให้มีการกำหนดข้อตกลง และความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอก โดยให้ครอบคลุมถึงผู้ให้บริการภายนอกที่รับจ้างช่วงจากผู้ให้บริการภายนอกหลักเป็นผู้จัดหา

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรควบคุมให้มีการกำหนดข้อตกลง และความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยให้ผู้ให้บริการภายนอกลงนามในหนังสือสัญญาการรักษาข้อมูลที่เป็นความลับ (Non-Disclosure Agreement) และให้ปฏิบัติตามระเบียบคำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบันโดยให้ครอบคลุมถึงผู้ให้บริการภายนอกที่รับจ้างช่วงจากผู้ให้บริการภายนอกหลักเป็นผู้จัดหา

นโยบาย

๑๑๙) ผู้รับผิดชอบสารสนเทศต้องติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของผู้ให้บริการภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรติดตามตรวจสอบรายงานหรือบันทึกการให้บริการของผู้ให้บริการภายนอกที่ให้บริการแก่หน่วยงานตามที่ว่าจ้างอย่างสม่ำเสมอ โดยมีแนวทางตามขั้นตอนปฏิบัติการบริหารจัดการผู้ให้บริการภายนอก (ภาคผนวก ๗)

นโยบาย

๑๒๐) กรณีที่ผู้ให้บริการภายนอกมีการเปลี่ยนแปลงกระบวนการ ขั้นตอน วิธีการปฏิบัติงาน การรักษาความมั่นคงปลอดภัยในการปฏิบัติงาน หน่วยงานที่เป็นคู่สัญญากับผู้ให้บริการภายนอกต้องประสานงานกับผู้ให้บริการภายนอกและให้มีการประเมินความเสี่ยงจากการเปลี่ยนแปลงดังกล่าว โดยต้องรายงานให้ผู้บริหารและผู้ที่เกี่ยวข้องรับทราบ รวมถึงให้กำหนดกระบวนการบริการจัดการความเสี่ยงดังกล่าวให้สอดคล้องเหมาะสม ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

หน่วยงานที่เป็นคู่สัญญากับผู้ให้บริการภายนอกควรปฏิบัติดังนี้

๑๒๐.๑ หากมีการปรับปรุงสัญญา หรือรายละเอียดการให้บริการควรได้รับการทบทวน และอนุมัติจากผู้บริหาร

๑๒๐.๒ กำหนดให้มีมาตรการเพื่อควบคุมการเปลี่ยนแปลงต่อระบบเทคโนโลยีสารสนเทศ เช่น การเปลี่ยนเทคโนโลยีใหม่ การติดตั้งผลิตภัณฑ์ใหม่ การปรับปรุงอุปกรณ์เครือข่าย การย้ายสถานที่ติดตั้งของระบบหรืออุปกรณ์ เป็นต้น

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรกำกับให้ผู้ให้บริการภายนอกปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งครอบคลุมถึงงานด้านความมั่นคงปลอดภัย ลักษณะการให้บริการและระดับการให้บริการ โดยมีแนวทางตามขั้นตอนปฏิบัติการบริหารจัดการผู้ให้บริการภายนอก (ภาคผนวก ๗)

หมวด ๑๒
การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

วัตถุประสงค์

เพื่อบริหารจัดการเหตุการณ์ไม่พึงประสงค์หรือไม่อาจคาดคิดด้านความมั่นคงปลอดภัยสารสนเทศให้ได้รับความเสียหายน้อยที่สุด จัดเก็บปัญหาที่เกิดขึ้น และเรียนรู้ข้อผิดพลาดมาปรับปรุงแก้ไขเพื่อป้องกันไม่ให้เกิดปัญหาซ้ำอีก

นโยบาย

๑๒๒) คณะกรรมการต้องกำหนดขอบเขตความรับผิดชอบของการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

นโยบาย

๑๒๓) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องรายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ผ่านช่องทางที่เหมาะสมโดยเร็วที่สุด โดยปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศและผู้ใช้ควรปฏิบัติดังนี้

๑๒๓.๑ รายงานสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด โดยเร็วที่สุด โดยให้

- ผู้ใช้แจ้งผ่าน PEA ITIL Service Desk โทร. ๐๒-๕๙๐-๙๙๖๐ หรือ ๙๙๖๐ Fax ๐๒-๐๐๙-๖๐๑๙ email servicedesk@pea.co.th
- ผู้รับผิดชอบสารสนเทศและหน่วยงานภายนอกองค์กรแจ้งผ่าน SOC (ผศม.) โดยผ่าน email soc@pea.co.th

๑๒๓.๒ รายงานข้อมูลรายละเอียดต่างๆ อย่างน้อยดังนี้

- ชื่อ - นามสกุล ของผู้แจ้ง
- สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด
- ข้อมูลสำหรับการติดต่อกลับ

นโยบาย

๑๒๔) ผู้ใช้ต้องบันทึกและรายงานจุดอ่อนใดๆ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้ใช้ต้องบันทึกรายงานจุดอ่อนด้านความมั่นคงปลอดภัยที่น่าสงสัย หรือสังเกตพบให้ผู้บังคับบัญชาและ/หรือผู้รับแจ้งเหตุ/หน่วยงานผู้รับผิดชอบ เช่น ซอฟต์แวร์ที่ใช้งานมีจุดอ่อน การรักษาความมั่นคงปลอดภัยทางกายภาพมีจุดอ่อน อุปกรณ์ที่นำมาใช้งานยังไม่ได้รับการตรวจประเมินช่องโหว่ (VA) อุปกรณ์ที่สำคัญไม่ได้รับการป้องกันที่ดี บุคคลอื่นสามารถเข้าถึงอุปกรณ์ได้โดยง่าย ไม่มีระบบสำรองไฟฟ้าที่ดี ไม่มีกล้อง CCTV ในจุดเสี่ยง ความซับซ้อนบางอย่างที่ผู้ใช้งานทั่วไปไม่ทราบ เป็นต้น โดยมีแนวทางตามขั้นตอนปฏิบัติการจัดการเหตุขัดข้อง (ภาคผนวก ๘)

นโยบาย

๑๒๕) ผู้รับผิดชอบสารสนเทศต้องมีการประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด โดยให้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรมีการประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด โดยมีแนวทางตามขั้นตอนปฏิบัติการจัดการเหตุขัดข้อง (ภาคผนวก ๘)

นโยบาย

๑๒๖) ผู้รับผิดชอบสารสนเทศต้องมีมาตรการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศที่ไม่พึงประสงค์หรือไม่อาจคาดคิด โดยมีแนวทางตามขั้นตอนปฏิบัติการจัดการเหตุขัดข้อง (ภาคผนวก ๘)

นโยบาย

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

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรรวบรวม จัดเก็บ และนำเสนอหลักฐาน หลังจากเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด โดยมีแนวทางตามขั้นตอนปฏิบัติการจัดการเหตุขัดข้อง เรื่องการเก็บรวบรวมหลักฐาน (ภาคผนวก ๘)

หมวด ๑๓
การบริหารจัดการด้านการบริการ หรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

วัตถุประสงค์

เพื่อระบุเหตุการณ์ที่อาจทำให้การให้บริการสารสนเทศหยุดชะงัก การบริหารจัดการในภาวะฉุกเฉินที่มีการคำนึงถึงความมั่นคงปลอดภัยสารสนเทศ ให้บริการสารสนเทศดำเนินไปได้อย่างต่อเนื่อง

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๒๙.๑ กำหนดให้มีการจัดทำบัญชีทรัพย์สินสำหรับกระบวนการทางธุรกิจสำคัญ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร ข้อมูล และบริการต่างๆ ที่สนับสนุนกระบวนการทางธุรกิจดังกล่าว รวมทั้งระบุระดับความสำคัญของทรัพย์สินเหล่านั้นด้วย

๑๒๙.๒ กำหนดให้มีการประเมินความเสี่ยงที่เกี่ยวข้องกับการสร้างความต่อเนื่องทางธุรกิจดังนี้

๑ ระบุเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้นและทำให้เกิดการหยุดชะงักต่อกระบวนการทางธุรกิจสำคัญ เช่น อุปกรณ์ทำงานล้มเหลว ไฟไหม้ น้ำท่วม การก่อการร้าย เป็นต้น

๒ ระบุโอกาสการเกิดขึ้นของเหตุการณ์เหล่านั้น

๓ วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักนั้น เช่น ความเสียหายทางการเงิน การสูญเสียส่วนแบ่งทางการตลาด การเสียชื่อเสียง ลูกค้าขาดความเชื่อมั่น เป็นต้น รวมทั้งระบุระดับของผลกระทบด้วย

๔ คำนวณค่าความเสี่ยงของเหตุการณ์เหล่านั้น

๑๒๙.๓ กำหนดให้มีการประเมินความเสี่ยงและจัดลำดับความเสี่ยง เพื่อกำหนดแผนหรือมาตรการลดความเสี่ยงตามลำดับความสำคัญของความเสี่ยงที่ได้ประเมินไว้

๑๒๙.๔ ปรับปรุงสัญญาการให้บริการโดยผู้ให้บริการภายนอกเพื่อให้ครอบคลุมการให้บริการเมื่อเกิดเหตุการณ์ฉุกเฉิน

๑๒๙.๕ กำหนดให้ผู้บริหารระดับสูงลงนามรับรองการสร้างความต่อเนื่อง

นโยบาย

๑๓๐) ผู้รับผิดชอบสารสนเทศและหน่วยงานที่เกี่ยวข้องต้องจัดทำข้อกำหนดเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ ที่จำเป็น โดยกำหนดให้เป็นส่วนหนึ่งของขั้นตอนการบริหารจัดการเพื่อการดำเนินงานอย่างต่อเนื่องในภาวะฉุกเฉิน ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศและหน่วยงานที่เกี่ยวข้องควรปฏิบัติดังนี้

๑๓๐.๑ กำหนดให้มีกระบวนการเพื่อสร้างความต่อเนื่องทางธุรกิจ (กระบวนการนี้จะช่วยให้กระบวนการทางธุรกิจสำคัญของ กฟภ. สามารถดำเนินต่อไปได้แม้จะมีเหตุหยุดชะงักที่รุนแรงก็ตาม เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การถูกปิดล้อมด้วยฝูงชน เป็นต้น)

๑๓๐.๒ กำหนดวัตถุประสงค์และขอบเขตของการสร้างความต่อเนื่องทางธุรกิจ

๑๓๐.๓ กำหนดหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับกระบวนการสร้างความต่อเนื่องทางธุรกิจ

๑๓๐.๔ กำหนดให้มีการระบุและจัดลำดับความสำคัญทางธุรกิจ

๑๓๐.๕ กำหนดให้มีงบประมาณและทรัพยากรอื่นๆ ที่จำเป็นสำหรับกระบวนการสร้างความต่อเนื่องทางธุรกิจ

๑๓๐.๖ ทดสอบแผนสร้างความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ

๑๓๐.๗ ปรับปรุงแผนสร้างความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ

๑๓๐.๘ ปลูกฝังวัฒนธรรมการสร้างความต่อเนื่องทางธุรกิจให้กับบุคลากร

๑๓๐.๙ กำหนดให้มีการรวมกระบวนการเพื่อสร้างความต่อเนื่องทางธุรกิจเข้าไว้เป็นส่วนหนึ่งของกระบวนการทางธุรกิจและโครงสร้างของ กฟภ.

นโยบาย

๑๓๑) ผู้รับผิดชอบสารสนเทศต้องกำหนดแผนกรณีมีเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงักเพื่อรักษาไว้หรือกู้คืนการให้บริการสารสนเทศ โดยคำนึงประเด็นความมั่นคงปลอดภัยสารสนเทศและให้สอดคล้องกับกลยุทธ์ความต่อเนื่องทางธุรกิจ ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๓๑.๑ แผนสร้างความต่อเนื่องทางธุรกิจควรครอบคลุมประเด็นสำคัญดังนี้

๑ วัตถุประสงค์ในการสร้างความต่อเนื่องทางธุรกิจ
๒ หน้าที่ความรับผิดชอบของบุคลากรทั้งหมดที่เกี่ยวข้อง
๓ ระยะเวลาที่นานที่สุดที่กระบวนการทางธุรกิจสำคัญเกิดการหยุดชะงักที่ยอมรับได้
๔ ระยะเวลาเป้าหมายในการกู้คืนกระบวนการทางธุรกิจสำคัญ
๕ ทรัพยากรที่จำเป็นต้องใช้ เช่น คน เวลา งบประมาณ สำหรับการกู้คืนกระบวนการทางธุรกิจสำคัญ
๖ บริการและระบบเทคโนโลยีสารสนเทศต่างๆ ที่จำเป็นต่อการกู้คืนกระบวนการทางธุรกิจสำคัญ
๗ ความสัมพันธ์ระหว่างกระบวนการทางธุรกิจทั้งภายในและภายนอก กฟภ. ที่เกี่ยวข้องกับกระบวนการทางธุรกิจสำคัญ (ความสัมพันธ์นี้จะช่วยให้เข้าใจว่าหากกระบวนการหนึ่งเกิดความเสียหายหรือหยุดชะงัก จะมีผลกระทบต่อกระบวนการอื่นอย่างไรบ้าง)
๘ ขั้นตอนปฏิบัติสำหรับการกู้คืนกระบวนการทางธุรกิจสำคัญและข้อมูลที่เกี่ยวข้องภายในระยะเวลาเป้าหมายที่ได้กำหนดไว้
๙ ผู้ให้บริการภายนอกที่เกี่ยวข้องกับกระบวนการทางธุรกิจสำคัญ
๑๐ สัญญาการให้บริการโดยผู้ให้บริการภายนอก
๑๑ การให้ความรู้แก่บุคลากรที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติตามแผนสร้างความต่อเนื่องที่ได้กำหนดไว้
๑๒ การทดสอบและปรับปรุงแผนสร้างความต่อเนื่องอย่างสม่ำเสมอ

๑๓๑.๒ กำหนดให้มีการจัดทำข้อตกลงการให้บริการโดยผู้ให้บริการภายนอก (สำหรับส่วนของกระบวนการทางธุรกิจสำคัญที่มีความเกี่ยวข้องกับผู้ให้บริการภายนอกนั้น)

๑๓๑.๓ กำหนดให้มีการรักษาความมั่นคงปลอดภัยทางกายภาพทั้งสำหรับสำนักงานหลักและสถานที่สำรองด้วยระดับความมั่นคงปลอดภัยที่เท่าเทียมกัน

๑๓๑.๔ จัดเก็บแผนสร้างความต่อเนื่องทางธุรกิจหรือสำเนาไว้นอกสถานที่ในระยะห่างที่เหมาะสม

๑๓๑.๕ ปรับปรุงแผนสร้างความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ

นโยบาย

๑๓๒) คณะกรรมการต้องกำหนดกรอบงาน (Framework) สำหรับการพัฒนาแผนการบริหารจัดการเพื่อการดำเนินงานทางธุรกิจมีความต่อเนื่องในภาวะฉุกเฉิน โดยคำนึงประเด็นความมั่นคงปลอดภัยสารสนเทศและให้สอดคล้องกับกลยุทธ์ความต่อเนื่องทางธุรกิจ

นโยบาย

๑๓๓) คณะกรรมการต้องจัดให้มีการฝึกซ้อม ทดสอบ และนำผลมาปรับปรุงแผนบริหารความต่อเนื่องให้เป็นปัจจุบันและมีประสิทธิผล

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๓๔.๑ ประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งานของระบบสารสนเทศสำรอง

๑๓๔.๒ กำกับให้มีการติดตั้งระบบสารสนเทศสำรอง หรืออุปกรณ์สำรอง หรือระบบสำหรับสนับสนุนการให้บริการ ที่เพียงพอ

หมวด ๑๔
การปฏิบัติตามกฎระเบียบ

วัตถุประสงค์

เพื่อให้ผู้ใช้ปฏิบัติตาม รวมถึงให้มีการตรวจสอบการปฏิบัติตามนโยบายทางด้านความมั่นคงปลอดภัยสารสนเทศที่กำหนดไว้ เพื่อให้การดำเนินงานของ กฟภ. เป็นไปตามกฎหมาย ระเบียบ ข้อตกลง สัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยต่างๆ

นโยบาย

๑๓๕) คณะกรรมการต้องรวบรวมกฎระเบียบ หลักเกณฑ์ และข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่มีความสอดคล้องกับกฎหมาย ข้อกำหนดตามสัญญาต่างๆ ของหน่วยงาน และจัดทำเป็นเอกสารเพื่อใช้เป็นข้อกำหนดในการปฏิบัติงานอย่างเป็นลายลักษณ์อักษร และมีการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

นโยบาย

๑๓๖) การใช้งานข้อมูลที่อาจถือเป็นทรัพย์สินทางปัญญาหรือการใช้งานซอฟต์แวร์ต้องมีความสอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่างๆ โดยให้ผู้รับผิดชอบสารสนเทศปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๓๖.๑ กำหนดให้มีการจัดซื้อซอฟต์แวร์จากแหล่งที่เชื่อถือได้เท่านั้น (ทั้งนี้ เพื่อให้ได้มาซึ่งซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย)

๑๓๖.๒ กำหนดให้มีการสร้างความตระหนักถึงสิทธิและทรัพย์สินทางปัญญาของผู้อื่น เช่น การใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้อง การไม่ละเมิดสิทธิและทรัพย์สินทางปัญญาของผู้อื่น ให้แก่พนักงาน

๑๓๖.๓ กำหนดให้มีการดำเนินการทางวินัย เมื่อพบว่าพนักงานมีการละเมิดนโยบายการป้องกันสิทธิและทรัพย์สินทางปัญญาที่ได้กำหนดไว้

๑๓๖.๔ จัดทำบัญชีทรัพย์สินซอฟต์แวร์และทรัพย์สินทางปัญญาอื่นๆ ที่หน่วยงานซื้อหรือจัดหามาใช้งาน (เช่น เอกสาร ข้อมูล) รวมทั้งระบุลิขสิทธิ์และข้อกำหนดต่างๆ ที่ผู้ใช้ต้องปฏิบัติตาม

๑๓๖.๕ กำหนดให้มีการตรวจสอบซอฟต์แวร์และทรัพย์สินทางปัญญาต่างๆ ที่หน่วยงานใช้งาน ว่ามีลิทสิทธิ์หรือมีใบอนุญาตการใช้งานอย่างถูกต้อง

๑๓๖.๖ กำหนดมาตรการควบคุมการใช้งานซอฟต์แวร์เพื่อให้ใช้งานไม่เกินตามจำนวนใบอนุญาตที่หน่วยงานได้รับ

๑๓๖.๗ กำหนดให้มีการติดตามเพื่อปรับปรุงหรือแก้ไขในเงื่อนไขการใช้งานของซอฟต์แวร์ที่หน่วยงานใช้งาน เช่น เมื่อมีการเปลี่ยนไปใช้งานซอฟต์แวร์เวอร์ชั่นที่ใหม่กว่า อาจมีการเปลี่ยนแปลงในเงื่อนไขการใช้งานได้ เป็นต้น

๑๓๖.๘ กำหนดให้มีการระมัดระวังการทำสำเนาหนังสือ บทความ รายงาน หรือเอกสารอื่นๆ ไม่ว่าจะเป็นบางส่วนหรือทั้งหมด ทั้งนี้เพื่อป้องกันการละเมิดลิขสิทธิ์

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๓๗.๑ กำหนดให้มีการจัดทำทะเบียนข้อมูลสารสนเทศที่สำคัญ ประเภทต่างๆ ของหน่วยงาน เช่น ข้อมูลทางบัญชี ข้อมูลบุคลากร ข้อมูล Log เป็นต้น

๑๓๗.๒ กำหนดให้มีการแยกหมวดหมู่ข้อมูลสารสนเทศที่สำคัญของหน่วยงานออกเป็นหมวดๆ เพื่อให้สามารถบริหารจัดการได้โดยง่ายและอย่างมั่นคงปลอดภัย

๑๓๗.๓ กำหนดระยะเวลาสำหรับการจัดเก็บข้อมูลสารสนเทศที่สำคัญแต่ละประเภท กล่าวคือ อย่างน้อยต้องจัดเก็บข้อมูลสารสนเทศที่สำคัญไว้จนกว่าจะครบระยะเวลาดังกล่าวจึงจะสามารถทำลายได้

๑๓๗.๔ กำหนดให้มีการจัดการกับสื่อบันทึกข้อมูลที่ใช้สำหรับการจัดเก็บข้อมูลสารสนเทศที่สำคัญให้สอดคล้องกับคำแนะนำและข้อกำหนดของผู้ผลิต เช่น ไม่เก็บไว้ในสถานที่ที่มีอุณหภูมิสูง เป็นต้น

๑๓๗.๕ กำหนดให้มีการป้องกันข้อมูลสารสนเทศที่สำคัญบนสื่อบันทึกข้อมูล จากการเสื่อมสภาพของสื่อบันทึกข้อมูล

๑๓๗.๖ กำหนดขั้นตอนปฏิบัติเพื่อใช้ในการทดสอบว่าข้อมูลอิเล็คทรอนิกส์สำคัญที่จัดเก็บไว้นั้น ยังคงเข้าถึงข้อมูลได้ตามปกติ

๑๓๗.๗ กำหนดให้มีการเลือกระบบหรือเทคโนโลยีที่เหมาะสมสำหรับการจัดเก็บข้อมูลสารสนเทศที่สำคัญเพื่อให้สามารถเข้าถึงได้อย่างรวดเร็วและมีประสิทธิภาพ

๑๓๗.๘ กำหนดให้มีการจัดเก็บข้อมูลสารสนเทศที่สำคัญไว้ตามระยะเวลาที่กฎหมาย ระเบียบข้อบังคับ หรือข้อกำหนดอื่นๆได้กำหนดไว้

๑๓๗.๙ กำหนดให้พนักงานสามารถทำลายข้อมูลสารสนเทศที่สำคัญได้ต่อเมื่อได้มีการจัดเก็บข้อมูลนั้นไว้ถึงระยะเวลาตามที่ได้กำหนดไว้และไม่มีความจำเป็นในการใช้งานอีกต่อไป

๑๓๗.๑๐ กำหนดแนวทางเพื่อควบคุมการจัดเก็บ ระยะเวลาการจัดเก็บการจัดการแหล่งที่มาของข้อมูล และการทำลายข้อมูล

๑๓๗.๑๑ กำหนดมาตรการป้องกันข้อมูลสารสนเทศที่สำคัญจากการสูญหาย ถูกทำลายหรือการปลอมแปลง

นโยบาย

๑๓๘) คณะกรรมการต้องจัดให้มีการคุ้มครองข้อมูลส่วนบุคคลโดยให้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่างๆ ของหน่วยงาน โดยให้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๓๙.๑ มีการพิจารณาข้อจำกัดในการใช้งานเทคโนโลยีการเข้ารหัสข้อมูลก่อนที่จะตัดสินใจนำมาใช้งาน

๑๓๙.๒ ขอคำแนะนำปรึกษาจากผู้รู้ว่าเทคนิคการเข้ารหัสลับที่ใช้สอดคล้องกับกฎหมายและข้อกำหนดตามสัญญาต่างๆ ของ กฟภ. หรือไม่

นโยบาย

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

นโยบาย

๑๔๑) ผู้บังคับบัญชาชั้นต้นขึ้นไปต้องกำกับดูแล ตรวจสอบ ให้พนักงานปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้บังคับบัญชาชั้นต้นขึ้นไปควรปฏิบัติดังนี้

๑๔๑.๑ กำกับดูแล ตรวจสอบ ให้พนักงานปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ของบุคคลากรใต้บังคับบัญชาอย่างสม่ำเสมอ

๑๔๑.๒ ถ้าตรวจพบการปฏิบัติงานที่ไม่สอดคล้องกับระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ซึ่งยังไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ต้องชี้แจงให้บุคคลากรใต้บังคับบัญชารับทราบและทำความเข้าใจ แต่หากความไม่สอดคล้องที่พบส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ ต้องดำเนินการลงโทษทางวินัยตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ.

นโยบาย

๑๔๒) ผู้รับผิดชอบสารสนเทศต้องทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับมาตรฐานการพัฒนางานด้านความมั่นคงปลอดภัยสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ.กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๔๒.๑ ทบทวนตรวจสอบระบบสารสนเทศในด้านเทคนิคอย่างสม่ำเสมอโดยใช้ซอฟต์แวร์หรือเครื่องมือต่างๆ

๑๔๒.๒ กำหนดให้ผู้ที่มีความเชี่ยวชาญทางเทคนิคเป็นผู้ดำเนินการตรวจสอบความสอดคล้องทางเทคนิค

๑๔๒.๓ กำหนดให้ผู้ที่มีความเชี่ยวชาญทางเทคนิคเป็นผู้ดำเนินการควบคุมการตรวจสอบความสอดคล้องทางเทคนิค

๑๔๒.๔ กำหนดให้มีการทดสอบการบุกรุกและการประเมินจุดอ่อนของระบบเทคโนโลยีสารสนเทศของ กฟภ. เป็นระยะๆ เพื่อค้นหาจุดอ่อนด้านความมั่นคงปลอดภัยของระบบเหล่านั้น (Penetration Testing) ทั้งนี้ควรบันทึกผลการทดสอบการบุกรุกและผลของการประเมินจุดอ่อนของระบบไว้เป็นลายลักษณ์อักษร

นโยบาย

๑๔๓) ผู้รับผิดชอบสารสนเทศต้องป้องกันมิให้มีการใช้งานระบบสารสนเทศผิดวัตถุประสงค์ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๔๓.๑ กำหนดให้มีการอนุมัติการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรก่อนที่จะเริ่มต้นใช้งาน ทั้งในส่วนของผู้ใช้ ผู้ให้บริการภายนอก และคู่สัญญาของ กฟภ.

๑๔๓.๒ กำหนดลักษณะหรือประเภทของการใช้งานที่ไม่อนุญาต ห้ามมิให้ใช้งาน หรือเป็นการใช้งานที่ผิดวัตถุประสงค์

๑๔๓.๓ กำหนดให้มีข้อความแจ้งเตือนบนหน้าจอภายหลังที่ล็อกอินสำเร็จเพื่อแสดงว่าระบบงานที่เข้าใช้งานเป็นทรัพย์สินของ กฟภ. และการใช้งานอนุญาตให้เฉพาะ ผู้ที่ได้รับอนุมัติแล้วเท่านั้น

๑๔๓.๔ แจ้งให้ผู้ใช้ได้ทราบถึงขอบเขตและวัตถุประสงค์ของการเข้าถึงระบบเทคโนโลยีสารสนเทศที่อนุญาตให้ใช้งาน รวมทั้งแจ้งให้ทราบว่าจะมีการเฝ้าระวัง เพื่อป้องกันการใช้ผิดวัตถุประสงค์

๑๔๓.๕ กำหนดให้มีการเฝ้าระวังการใช้งานในลักษณะที่ผิดวัตถุประสงค์

๑๔๓.๖ กำหนดให้มีการรายงานต่อผู้บังคับบัญชาในกรณีที่พบการใช้งานที่ผิดวัตถุประสงค์

๑๔๓.๗ กำหนดให้มีการดำเนินการทางวินัยและ/หรือทางกฎหมาย ในกรณีที่พบว่ามีการใช้งานระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์

นโยบาย

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

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

๑๔๔.๑ กำหนดให้มีการแยกการติดตั้งเครื่องมือที่ใช้เพื่อการตรวจสอบ เช่น แยกการติดตั้งซอฟต์แวร์ที่ใช้สแกนช่องโหว่ของระบบสารสนเทศออกจากเครื่องให้บริการ หรือเครื่องที่ใช้ในการพัฒนา

๑๔๔.๒ กำหนดให้มีการจัดเก็บและป้องกันเครื่องมือที่ใช้ในการตรวจสอบ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

ประกาศนี้ให้มีผลใช้บังคับตั้งแต่วันที่ ๑๙ ส.ค. ๒๕๖๒ เป็นต้นไป

ประกาศ ณ วันที่ ๑๙ ส.ค. ๒๕๖๒

(นายสมพงษ์ ปรีเปรม)
ผู้ว่าการการไฟฟ้าส่วนภูมิภาค

ตารางภาคผนวก

ของแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ

ประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๒

ข้อ	ภาคผนวก
๑	ระเบียบการไฟฟ้าส่วนภูมิภาคว่าด้วยการจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ
๒	ขั้นตอนปฏิบัติการจัดระดับชั้นข้อมูล
๓	ขั้นตอนปฏิบัติการทำลายสื่อบันทึกข้อมูล
๔	ขั้นตอนปฏิบัติการควบคุมการเข้า-ออกพื้นที่ศูนย์คอมพิวเตอร์
๕	แนวทางปฏิบัติเรื่องการใช้พื้นที่ศูนย์คอมพิวเตอร์
๖	ขั้นตอนปฏิบัติการควบคุมการติดตั้งซอฟต์แวร์
๗	ขั้นตอนปฏิบัติการบริหารจัดการผู้ให้บริการภายนอก
๘	ขั้นตอนปฏิบัติการจัดการเหตุขัดข้อง

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 ๙
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 โดยได้รับความเห็นชอบจากผู้รับผิดชอบสารสนเทศเพื่อลดความเสี่ยงในการเกิดการหยุดชะงักของกระบวนการทางธุรกิจ

๘๘) คณะกรรมการต้องกำหนดประเภทข้อมูลตามลำดับชั้นความลับเพื่อให้ผู้รับผิดชอบสารสนเทศและผู้ใช้ถือปฏิบัติตาม เพื่อเป็นการป้องกันไม่ให้มีการเข้าถึงข้อมูลหรือเอกสารเกี่ยวกับระบบสารสนเทศ (System documentation) โดยไม่ได้รับอนุญาต

๘๙) คณะกรรมการต้องกำหนดนโยบายและขั้นตอนการปฏิบัติ เพื่อป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยน หรือใช้ข้อมูลร่วมกัน ผ่านระบบสารสนเทศที่มีการเชื่อมต่อระหว่างระบบสารสนเทศต่างๆ

หมวด ๙
ความมั่นคงปลอดภัยด้านเครือข่าย

วัตถุประสงค์

เพื่อควบคุมการบริหารจัดการเครือข่ายคอมพิวเตอร์ทั้งภายในและภายนอก กฟภ. รวมถึงการควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศกับหน่วยงานภายนอกให้มีความมั่นคงปลอดภัย

แนวนโยบาย

๙๐) ผู้ดูแลระบบสารสนเทศต้องบริหารจัดการ การควบคุมเครือข่ายคอมพิวเตอร์ เครือข่ายสื่อสารเพื่อป้องกันภัยคุกคาม 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 ...

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 โดยคำนึงประเด็นความมั่นคงปลอดภัยสารสนเทศ และให้สอดคล้องกับกลยุทธ์ความต่อเนื่องทางธุรกิจ

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