



การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

สรก.(ดส)
เลขที่รับ 1203
วันที่ 1 เม.ย. 2568

ฟสท.
เลขรับ 1084
วันที่ 27 มี.ค. 2568

ผู้ว่าการ
วันที่ 21 เม.ย. 2568
เลขที่รับ 1274

สชก (ดส-พ)
วันที่ 27 มี.ค. 2568
เลขรับ 1018

จาก คณะอนุกรรมการจัดทำ ทบทวนฯ ถึง ฟสท.
เลขที่ กมม.(สม) 366 /2568 วันที่ 27 มี.ค. 2568
เรื่อง ขออนุมัติใช้และลงนามนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
พ.ศ. 2568

เรียน อฟ.สท.

1. เรื่องเดิม

1.1 ตามประกาศการไฟฟ้าส่วนภูมิภาค เรื่อง มาตรการการใช้ทรัพย์สินสารสนเทศของ กฟผ. พ.ศ. 2563 ประกาศ ณ วันที่ 6 สิงหาคม 2563 (เอกสารแนบ 1) เพื่อเป็นการป้องกันภัยคุกคามที่อาจเกิดขึ้นกับระบบสารสนเทศของ กฟผ. รวมทั้งเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพย์สินสารสนเทศของ กฟผ.

1.2 ตามอนุมัติ ผวก. ลงวันที่ 24 มกราคม 2566 (หนังสือเลขที่ กมม.(สม) 60/2566 ลงวันที่ 16 มกราคม 2566) เรื่องขออนุมัติใช้นโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ พ.ศ. 2566 และแนวทางปฏิบัติการใช้บริการคลาวด์ พ.ศ. 2566 และขออนุมัติยกเลิกนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. 2561 นโยบายความมั่นคงปลอดภัยสารสนเทศ (ฉบับที่ 2) พ.ศ. 2562 แนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. 2562 (เอกสารแนบ 2)

1.3 ตามคำสั่งการไฟฟ้าส่วนภูมิภาค ที่ พ.(ก) 369/2567 สั่ง ณ วันที่ 22 มีนาคม 2567 เรื่องแต่งตั้งคณะอนุกรรมการจัดทำ ทบทวน ปรับปรุง แก้ไข นโยบาย แนวทางปฏิบัติ และมาตรการการจัดการความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ (เอกสารแนบ 3) มีอำนาจหน้าที่ตามข้อ 1) จัดทำ ทบทวน ปรับปรุง แก้ไข นโยบาย แนวทางปฏิบัติ และมาตรการ การจัดการ และความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์ และข้อ 5) นำเสนอคณะกรรมการ การจัดการและความมั่นคงปลอดภัยด้านสารสนเทศ พิจารณา ขออนุมัติใช้นโยบาย แนวทางปฏิบัติ และมาตรการ การจัดการความมั่นคงปลอดภัยด้านสารสนเทศและไซเบอร์

1.4 ตามคำสั่ง ...

1.4 ตามคำสั่งการไฟฟ้าส่วนภูมิภาค ที่ พ.ก) 1487/2567 สั่ง ณ วันที่ 27 ธันวาคม 2567 เรื่อง แต่งตั้งคณะกรรมการกำกับดูแลและขับเคลื่อนองค์กรด้วยดิจิทัลของ กฟภ. (PEA Digital Transformation Governance Committee) คณะกรรมการฯ มีอำนาจหน้าที่ ข้อ 4) พิจารณานโยบาย ระเบียบ แนวปฏิบัติ และการประเมินความเสี่ยง ที่เกี่ยวข้องด้านเทคโนโลยีดิจิทัลและความมั่นคงปลอดภัยไซเบอร์ (เอกสารแนบ 4)

2. ข้อเท็จจริง

2.1 ตามหนังสือเลขที่ กมม.(สม) 138/2568 ลงวันที่ 14 กุมภาพันธ์ 2568 เรื่อง ขอนำเรื่องนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ พ.ศ. 2568 เข้าคณะกรรมการกำกับดูแลและขับเคลื่อนองค์กรด้วยดิจิทัลของ กฟภ. (PEA Digital Transformation Governance Committee) เพื่อพิจารณา (เอกสารแนบ 5)

2.2 ตามรายงานการประชุมคณะกรรมการกำกับดูแลและขับเคลื่อนองค์กรด้วยดิจิทัลของ กฟภ. (PEA Digital Transformation Governance Committee) ครั้งที่ 1/2568 เมื่อวันที่ 6 มีนาคม 2568

วาระที่ 2.1 นโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ พ.ศ. 2568 โดยที่ประชุมมีมติเห็นชอบผลการทบทวนนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ พ.ศ. 2568 (เอกสารแนบ 6)

2.3 คณะอนุกรรมการฯ ได้ดำเนินการปรับแก้ไขตามข้อสังเกตของคณะกรรมการกำกับดูแลและขับเคลื่อนองค์กรด้วยดิจิทัลของ กฟภ. (PEA Digital Transformation Governance Committee) และจัดทำนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ พ.ศ. 2568 (เอกสารแนบ 7)

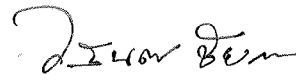
3. ข้อพิจารณา

เพื่อให้ กฟภ. มีการกำหนดนโยบายและให้การสนับสนุนด้านการจัดการความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ และเป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และสามารถนำไปปฏิบัติใช้กับองค์กรให้เกิดประโยชน์สูงสุดในด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ คณะอนุกรรมการฯ ได้พิจารณาแล้วจึงเห็นควรขอดำเนินการ ดังนี้

- 3.1 อนุมัติยกเลิกมาตรการการใช้ทรัพย์สินสารสนเทศ ของ กฟภ. พ.ศ. 2563 ตามข้อ 1.1
- 3.2 อนุมัติยกเลิกนโยบายความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ พ.ศ. 2566 ตามข้อ 1.2
- 3.3 อนุมัติใช้และลงนามนโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ พ.ศ. 2568 ตามข้อ 2.3

4. ข้อเสนอ

จึงเรียนมาเพื่อโปรดพิจารณา หากเห็นชอบโปรดนำเรียน รพก.(ดส) พิจารณานำเรียน ผวก. อนุมัติและลงนามตามข้อ 3.1 - 3.3 ต่อไป พร้อมนี้ได้แนบรายละเอียดเอกสารที่เกี่ยวข้องมาเพื่อประกอบการ พิจารณาด้วยแล้ว



(นายวสันต์ ชัยพร)

รพ.สท.

ประธานอนุกรรมการจัดทำ ทบทวน ปรับปรุง แก้ไข นโยบาย
แนวทางปฏิบัติ และมาตรการ การจัดการความมั่นคงปลอดภัย
ด้านสารสนเทศและไซเบอร์

เรียน รพก.(ดส) ผ่าน ผชก.(ดส-พ) 31 มี.ค. 2568

เพื่อโปรดพิจารณา หากเห็นชอบโปรดนำ
เรียน ผวก. อนุมัติและลงนามตามข้อ 3.1 - 3.3
ตามที่คณะอนุกรรมการฯ เสนอต่อไป



(นางสุทธีรธรรม มารัตน์)

อ.พ.สท.

27 มี.ค. 2568

อนุมัติตามเสนอ-ลงนามแล้ว



นายสุกษม ชัยพร
ผวก.

เรียน ผวก. 10 เม.ย. 2568

เพื่อโปรดพิจารณาอนุมัติและลงนามตามข้อ
3.1 - 3.3 ตามที่คณะอนุกรรมการฯ เสนอต่อไป



(นายวิโรจน์ บัวคี่)

รพก.(ดส)

- 1 เม.ย. 2568

ผล.ม.



(นางสาววิภาดา คุณะศรี)

อ.ก.พ.ผ.

11 เม.ย. 2568

ก.พ.ม.



(นางสุทธีรธรรม มารัตน์)

อ.พ.สท.

11 เม.ย. 2568

- ผชก.(ดส-พ)

- ผล.ม.

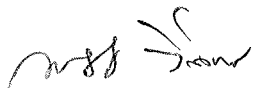


(นายวิโรจน์ บัวคี่)

รพก.(ดส)

10 เม.ย. 2568

ผสม. ก.ม.ม.
โทร.6135





การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

นโยบายและแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศและไซเบอร์
พ.ศ. 2568

สารบัญ

	หน้า
คำนิยาม	3
หมวด 1 นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ	6
หมวด 2 การจัดโครงสร้างด้านความมั่นคงปลอดภัยสารสนเทศ	6
หมวด 3 ความมั่นคงปลอดภัยสารสนเทศด้านบุคลากร	11
หมวด 4 การบริหารจัดการทรัพยากรสารสนเทศ	14
หมวด 5 การควบคุมการเข้าถึง	19
หมวด 6 การควบคุมการเข้ารหัสลับข้อมูล	29
หมวด 7 ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม	31
หมวด 8 ความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน	39
หมวด 9 ความมั่นคงปลอดภัยด้านเครือข่าย	51
หมวด 10 ความมั่นคงปลอดภัยในการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ	54
หมวด 11 การจัดการความสัมพันธ์กับผู้ให้บริการภายนอก	66
หมวด 12 การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด	68
หมวด 13 การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง	72
หมวด 14 การปฏิบัติตามกฎระเบียบ	75

9. ความรับผิดชอบสำหรับกรณีที่ข้อมูลที่แลกเปลี่ยนกันเกิดการสูญหายหรือเกิดเหตุการณ์ความเสียหายอื่น ๆ กับข้อมูลนั้น
10. ปฏิบัติตามเงื่อนไขต่าง ๆ ที่จะต้องปฏิบัติตาม เช่น กฎหมายลิขสิทธิ์ ใบอนุญาตการใช้งานซอฟต์แวร์ (Software License) เป็นต้น

นโยบาย

96) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic Messaging) ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศและผู้ใช้ควรปฏิบัติดังนี้

- 96.1 ในการส่งข้อมูลที่เป็นความลับ เช่น ข้อมูลเงินเดือน ต้องเข้ารหัสข้อมูล และห้ามส่งรหัสผ่านไปกับข้อมูล เป็นต้น
- 96.2 ไม่เขียนหรือพิมพ์ข้อความที่ไม่เหมาะสม หรือไม่ทำการใด ๆ ที่มีความเสี่ยงต่อการละเมิดพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

นโยบาย

97) คณะกรรมการต้องกำหนด และทบทวน ข้อตกลงการรักษาข้อมูลที่เป็นความลับ (Confidentiality Agreement หรือ Non-Disclosure Agreement) ให้กับสอดคล้องกับสถานการณ์และความต้องการของ กฟผ. ในการปกป้องข้อมูลสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อใช้ประกอบสัญญาตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

หมวด 10

ความมั่นคงปลอดภัยในการจัดหา พัฒนา และบำรุงรักษาระบบสารสนเทศ

วัตถุประสงค์

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

นโยบาย

98) หน่วยงานที่มีการจัดหาหรือจัดให้มีการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิม ต้องระบุความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบงานที่พัฒนาขึ้นมาใช้งาน นับตั้งแต่เริ่มต้นออกแบบระบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

หน่วยงานที่มีการจัดหาหรือจัดให้มีการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงระบบสารสนเทศเดิมควรปฏิบัติดังนี้

- 98.1 ประเมินความเสี่ยงสำหรับระบบงานที่จะจัดหาหรือพัฒนาขึ้นมาใช้งาน และระบุข้อกำหนดด้านความมั่นคงปลอดภัยที่ต้องมีหรือปฏิบัติเพื่อลดความเสี่ยงที่ได้ประเมิน
- 98.2 ระบุข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับระบบงานที่จะจัดหาหรือพัฒนาขึ้นมาใช้งาน นับตั้งแต่เริ่มต้นออกแบบระบบ
- 98.3 ระบุข้อกำหนดด้านความมั่นคงปลอดภัยสำหรับซอฟต์แวร์ที่จะจัดซื้อหรือจัดหา มาใช้งาน
- 98.4 พิจารณาความสำคัญของข้อมูล ในระบบงานที่จะพัฒนาหรือจัดหา มาใช้งาน และระบุข้อกำหนดด้านความมั่นคงปลอดภัยที่เหมาะสมเพื่อป้องกันข้อมูลนั้น
- 98.5 ทดสอบเพื่อประเมินซอฟต์แวร์หรือระบบงานที่จัดหา มาใช้งานว่าตรงตามข้อกำหนดด้านความมั่นคงปลอดภัยที่ระบุไว้หรือไม่
- 98.6 ทำสัญญา และระบุข้อกำหนดด้านความมั่นคงปลอดภัยให้ผู้พัฒนาหรือผู้จัดหา ภายนอกปฏิบัติตาม
- 98.7 พิจารณาปิดการใช้งานฟังก์ชันเพิ่มเติมหรือที่ไม่มีความจำเป็นต่อการใช้งานของซอฟต์แวร์ที่จัดซื้อหรือจัดหา มาใช้งาน ทั้งนี้เพื่อลดความเสี่ยงอันเนื่องมาจากฟังก์ชันดังกล่าว

นโยบาย

99) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องป้องกันข้อมูลสารสนเทศที่มีการแลกเปลี่ยนในการทำพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce) ผ่านเครือข่ายคอมพิวเตอร์สาธารณะ เพื่อมิให้มีการฉ้อโกง ละเมิดสัญญา หรือมีการรั่วไหล หรือข้อมูลสารสนเทศถูกแก้ไขโดยมิได้รับอนุญาต ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

- 99.1 กำหนดมาตรการการพิสูจน์ตัวตนสำหรับผู้เข้าใช้ระบบงานพาณิชย์อิเล็กทรอนิกส์ ที่มีความมั่นคงปลอดภัยเพียงพอ
- 99.2 กำหนดมาตรการป้องกันข้อมูลลับ ข้อมูลสำคัญ หรือข้อมูลส่วนบุคคลในระบบงานพาณิชย์อิเล็กทรอนิกส์

- 99.3 กำหนดวิธีการตรวจสอบข้อมูลการชำระเงินของลูกค้า กล่าวคือ กฟภ.จะสามารถตรวจสอบได้ว่าลูกค้าได้ชำระเงินแล้วหรือไม่ หรือในทางกลับกัน ลูกค้าสามารถตรวจสอบได้ว่า กฟภ. ได้รับเงินค่าสินค้าแล้วหรือไม่
- 99.4 กำหนดให้มีการระบุถึงความรับผิดชอบของ กฟภ. กรณีที่มีการฉ้อโกงเกิดขึ้นกับธุรกรรมทางอิเล็กทรอนิกส์ของลูกค้า
- 99.5 กำหนดมาตรการการป้องกันข้อมูล เช่น การเข้ารหัสข้อมูล เพื่อป้องกันกิจกรรมการทำธุรกรรมทางอิเล็กทรอนิกส์ของลูกค้า เป็นต้น
- 99.6 ปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และที่แก้ไขเพิ่มเติม

นโยบาย

100) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องป้องกันไม่ให้มีการแก้ไขเปลี่ยนแปลงข้อมูลสารสนเทศ โดยไม่ได้รับอนุญาตและรักษาความถูกต้องครบถ้วนของข้อมูลสารสนเทศ ที่มีการเผยแพร่ต่อสาธารณชน ถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

- 100.1 กำหนดให้มีการป้องกันข้อมูลหรือซอฟต์แวร์ที่สำคัญที่ปรากฏในระบบงานสาธารณะ เช่น บนเว็บไซต์จากการถูกเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต เป็นต้น
- 100.2 กำหนดให้มีการประเมินความเสี่ยงต่อระบบงานสาธารณะและข้อมูลสำคัญในระบบ และกำหนดมาตรการลดความเสี่ยงก่อนที่จะเริ่มเปิดให้บริการระบบดังกล่าว
- 100.3 กำหนดให้มีกระบวนการตรวจสอบความถูกต้องและเหมาะสม และอนุมัติข้อมูลก่อนที่จะทำการเผยแพร่ข้อมูลนั้นในระบบงานสาธารณะ
- 100.4 กำหนดมาตรการป้องกันเพื่อไม่ให้ผู้ที่สามารถใช้งานระบบงานสาธารณะสามารถใช้ระบบนี้เป็นทางผ่านไปสู่เครือข่ายอื่น ๆ ที่เชื่อมต่อกับระบบงานนี้

นโยบาย

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

แนวทางปฏิบัติ

หน่วยงานที่เกี่ยวข้องในการทำธุรกรรมทางออนไลน์ควรปฏิบัติดังนี้

- 101.1 กำหนดให้มีการใช้ลายมือชื่ออิเล็กทรอนิกส์ เพื่อป้องกันธุรกรรมทางอิเล็กทรอนิกส์ที่มีความสำคัญ เช่น ป้องกันจากการถูกสวมรอยทำธุรกรรมแทนเจ้าตัว เป็นต้น
- 101.2 กำหนดให้มีกระบวนการบริหารจัดการการใช้ลายมือชื่ออิเล็กทรอนิกส์ การออกหรือการใช้ใบรับรองอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัย

- 101.3 กำหนดมาตรการการการพิสูจน์ตัวตนสำหรับผู้เข้าทำธุรกรรมทางอิเล็กทรอนิกส์ที่มีความมั่นคงปลอดภัยเพียงพอ
- 101.4 กำหนดให้มีการเข้ารหัสข้อมูลและหรือใช้โพรโตคอลที่มีความมั่นคงปลอดภัยสำหรับข้อมูลที่จะมีการส่งผ่านเครือข่ายหรือระบบสื่อสารระหว่างลูกค้ากับระบบงานให้บริการธุรกรรมทางอิเล็กทรอนิกส์
- 101.5 กำหนดให้มีการจัดเก็บข้อมูลธุรกรรมทางอิเล็กทรอนิกส์ไว้บนสื่อบันทึกข้อมูลที่ไม่สามารถเข้าถึงได้โดยผู้อื่น รวมทั้งควรจัดเก็บไว้เพื่อไม่ให้อ่านเข้าถึงได้โดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เป็นต้น

นโยบาย

102) ผู้พัฒนาระบบสารสนเทศต้องพัฒนาซอฟต์แวร์และระบบสารสนเทศอย่างมั่นคงปลอดภัยตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรปฏิบัติดังนี้

- 102.1 สภาพแวดล้อมในการพัฒนาฯ ควรมีความมั่นคงปลอดภัย เช่น สถานที่ ระบบคอมพิวเตอร์ ระบบเครือข่าย ฐานข้อมูล ซอฟต์แวร์ เป็นต้น
- 102.2 เขียนโปรแกรมแต่ละภาษา ให้ปลอดภัย (Secure Coding)
- 102.3 มีจุดตรวจความมั่นคงปลอดภัยในแต่ละขั้นตอนหลักในโครงการพัฒนาระบบสารสนเทศ
- 102.4 ที่เก็บข้อมูลและส่วนประกอบของการพัฒนาซอฟต์แวร์ควรมีความปลอดภัย
- 102.5 มีความมั่นคงปลอดภัยสำหรับระบบที่จัดการการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์หนึ่งหรือหลายไฟล์ (Version Control) เช่น ให้ผู้มีสิทธิเท่านั้น จัดเก็บไว้ในที่ปลอดภัย เป็นต้น
- 102.6 ปิดช่องโหว่ และควบคุมไม่ให้ช่องโหว่นั้นกลายเป็นจุดอ่อนของระบบ

นโยบาย

103) ผู้พัฒนาระบบสารสนเทศต้องมีขั้นตอนการควบคุมการเปลี่ยนแปลงระบบสารสนเทศเป็นลายลักษณ์อักษร เพื่อควบคุมให้ระบบเป็นไปตามข้อตกลงที่กำหนดไว้และมีความมั่นคงปลอดภัยตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรปฏิบัติดังนี้

- 103.1 กำหนดขั้นตอนการควบคุมการเปลี่ยนแปลงระบบสารสนเทศเป็นลายลักษณ์อักษร (การเปลี่ยนแปลงดังกล่าวครอบคลุมถึง การขอให้พัฒนาหรือปรับปรุงระบบงานเพิ่มเติมตามคำขอ การเปลี่ยนแปลงฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น)

103.2 ขั้นตอนปฏิบัติฯ ควรครอบคลุมประเด็นดังนี้

1. กำหนดผู้ทำหน้าที่ขออนุมัติการเปลี่ยนแปลง และผู้มีอำนาจอนุมัติการเปลี่ยนแปลงนั้น
2. กำหนดให้มีการชี้แจงเหตุผลของการขอเปลี่ยนแปลงนั้น
3. กำหนดให้มีการพิจารณาผลกระทบและความเร่งด่วนในการดำเนินการ
4. กำหนดให้มีการระบุรายละเอียดของสิ่งที่จะดำเนินการเปลี่ยนแปลง เช่น การเปลี่ยนแปลงต่อ ซอฟต์แวร์ ฮาร์ดแวร์ ฐานข้อมูล เป็นต้น
5. กำหนดให้มีการวางแผนและดำเนินการทดสอบตามความจำเป็น
6. กำหนดให้มีการติดตั้งจริงภายหลังการทดสอบเสร็จ
7. กำหนดให้มีการรายงานผลภายหลังการติดตั้ง

103.3 ในการขออนุมัติการเปลี่ยนแปลงระบบงาน กฟภ. ควรกำหนดให้ผู้ที่เกี่ยวข้องปฏิบัติดังนี้

1. พิจารณาความเสี่ยงที่มีต่อระบบงาน (สำหรับการเปลี่ยนแปลงที่จะดำเนินการนั้น) และกำหนดมาตรการลดความเสี่ยงที่จำเป็นก่อนที่จะดำเนินการเปลี่ยนแปลง
2. พิจารณาผลกระทบที่มีต่อระบบงาน เช่น การเปลี่ยนแปลงนั้นอาจส่งผลให้เกิดการหยุดชะงักต่อกระบวนการทางธุรกิจสำคัญ เป็นต้น
3. กำหนดมาตรการป้องกันที่จำเป็นเพื่อรองรับต่อการเปลี่ยนแปลงดังกล่าว
4. ระมัดระวังเพื่อไม่ให้เกิดการเปลี่ยนแปลงที่จะดำเนินการนั้นไปทำให้มาตรการหรือขั้นตอนปฏิบัติด้านความมั่นคงปลอดภัยที่มีอยู่แล้วเดิมเกิดความเสียหายหรือทำให้เกิดการละเมิดความมั่นคงปลอดภัยได้
5. ควบคุมการเข้าถึงของผู้พัฒนาระบบสารสนเทศโดยกำหนดให้สามารถเข้าถึงได้เฉพาะในส่วนของเครื่องสำหรับทำการพัฒนาระบบ ระบบงานไดเรกทอรีที่จำเป็นต่อการปฏิบัติงานของผู้พัฒนาระบบสารสนเทศนั้นเท่านั้น
6. ทดสอบระบบงานโดยผู้ใช้อย่างครอบคลุมและกำหนดให้ผู้ใช้นามรับรองการใช้งาน
7. ดำเนินการปรับปรุงเอกสารต่าง ๆ ที่เกี่ยวข้องกับระบบงานให้มีความทันสมัย เช่น เอกสารคู่มือการใช้งาน เอกสารวิเคราะห์และออกแบบระบบ เป็นต้น
8. บันทึกข้อมูลที่เกี่ยวข้องกับการขออนุมัติการเปลี่ยนแปลงนั้นไว้ เพื่อเอาไว้ใช้ในการเรียนรู้ในภายหลังหรือ เป็นหลักฐานในการตรวจสอบในภายหลังได้

นโยบาย

104) กรณีมีการเปลี่ยนแปลงต่อระบบปฏิบัติการคอมพิวเตอร์ของระบบสารสนเทศ ให้ผู้พัฒนาระบบสารสนเทศทดสอบและทบทวนระบบสารสนเทศนั้น เพื่อให้มั่นใจได้ว่าไม่มีผลกระทบต่อการปฏิบัติงานกับระบบและด้านความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรปฏิบัติดังนี้

- 104.1 กรณีมีการเปลี่ยนแปลงต่อระบบปฏิบัติการคอมพิวเตอร์ของระบบสารสนเทศ (ซึ่งรวมถึงการติดตั้งระบบปฏิบัติการเวอร์ชันใหม่ และการติดตั้งโปรแกรมแก้ไขช่องโหว่ของระบบปฏิบัติการ) กฟผ. ควรกำหนดให้มีการวางแผนเพื่อดำเนินการเปลี่ยนแปลงนั้น รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในการดำเนินการ
- 104.2 กำหนดให้มีการแจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการดำเนินการเปลี่ยนแปลงระบบปฏิบัติการนั้น
- 104.3 กำหนดให้มีการทดสอบระบบงานที่จะมีการเปลี่ยนแปลงระบบปฏิบัติการให้ครอบคลุม ก่อนที่จะดำเนินการเปลี่ยนแปลงนั้น
- 104.4 กำหนดให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่ได้เปลี่ยนแปลงระบบปฏิบัติการไปแล้ว เพื่อติดตามความสมบูรณ์ของการทำงาน และดูว่ามีผลกระทบต่อมาตรการความมั่นคงปลอดภัยของระบบงานนั้นหรือไม่

นโยบาย

105) ผู้รับผิดชอบสารสนเทศต้องจำกัดการเปลี่ยนแปลงใด ๆ ต่อซอฟต์แวร์สำเร็จรูปที่ใช้งาน (Software Package) โดยให้เปลี่ยนแปลงเฉพาะเท่าที่จำเป็นและควบคุมทุก ๆ การเปลี่ยนแปลงอย่างเข้มงวด เพื่อป้องกันการละเมิดลิขสิทธิ์ เพื่อความมั่นคงปลอดภัยของซอฟต์แวร์สำเร็จรูป เพื่อป้องกันผลกระทบที่ กฟผ. อาจต้องรับผิดชอบต่อการบำรุงรักษาซอฟต์แวร์นั้นด้วยตนเองต่อไปในอนาคต โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

- 105.1 ในกรณีที่จำเป็นต้องปรับปรุงหรือเปลี่ยนแปลงต่อซอฟต์แวร์สำเร็จรูปที่ใช้งาน (Software Package) ควรปฏิบัติดังนี้
 1. ตรวจสอบเงื่อนไขหรือข้อตกลงการใช้งานก่อนว่าจำเป็นต้องได้รับการอนุมัติจากผู้ผลิตซอฟต์แวร์ก่อนดำเนินการเปลี่ยนแปลงใด ๆ หรือไม่ ทั้งนี้เพื่อป้องกันการละเมิดลิขสิทธิ์
 2. พิจารณาหรือตรวจสอบว่าการเปลี่ยนแปลงนั้นจะก่อให้เกิดความเสียหายต่อมาตรการความมั่นคงปลอดภัยของซอฟต์แวร์นั้นหรือไม่
- 105.2 กำหนดให้มีการประสานงานกับเจ้าของลิขสิทธิ์ในซอฟต์แวร์ เพื่อให้การเปลี่ยนแปลงที่ได้ดำเนินไปนั้นได้รับการตอบรับเพื่อบรรจุไว้เป็นส่วนหนึ่งของซอฟต์แวร์สำเร็จรูปที่ใช้งาน (Software Package) นั้น เช่น ในเวอร์ชันถัดไป รวมทั้งกำหนดให้มีการพิจารณาผลกระทบที่ กฟผ. อาจต้องรับผิดชอบต่อการบำรุงรักษาซอฟต์แวร์นั้นด้วยตนเองต่อไปในอนาคต
- 105.3 กำหนดให้มีการปรับปรุงหรือเปลี่ยนแปลงต่อซอฟต์แวร์สำเร็จรูปที่เป็นฉบับสำเนา และเก็บตัวต้นฉบับไว้ในสภาพเดิม

- 105.4 กำหนดให้มีการทดสอบซอฟต์แวร์สำเร็จรูปที่ได้ทำการปรับปรุงหรือแก้ไขเองนั้นให้ครอบคลุมก่อนที่จะดำเนินการติดตั้ง
- 105.5 กำหนดให้มีการบันทึกกลายลักษณ์อักษรเกี่ยวกับรายละเอียดของการปรับปรุงหรือเปลี่ยนแปลงต่อซอฟต์แวร์สำเร็จรูปนั้น เพื่อในกรณีที่จำเป็นต้องดำเนินการเพิ่มเติมอีกในอนาคต จะได้ทราบรายละเอียดการดำเนินการที่ได้ทำไปแล้ว
- 105.6 กำหนดให้มีหน่วยงานภายนอกอิสระหรือผู้ที่มีความรู้ความสามารถในการประเมินซอฟต์แวร์ทำหน้าที่ในการประเมินซอฟต์แวร์สำเร็จรูปที่ กพท. ได้ทำการปรับปรุงเอง

นโยบาย

106) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องพัฒนาและติดตั้งใช้งานระบบสารสนเทศโดยคำนึงถึงหลักการความมั่นคงปลอดภัย ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

- 106.1 ให้สิทธิต่ำที่สุด (Least Privilege) แก่ผู้ใช้ เพื่อป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต
- 106.2 ให้สิทธิเฉพาะที่จำเป็นในการปฏิบัติงาน (Need to Know) แก่ผู้ใช้เพื่อป้องกันการรั่วไหลของข้อมูลสำคัญ
- 106.3 พัฒนาระบบสารสนเทศในลักษณะเปิด (Open Design) เพื่อให้การพัฒนาระบบสารสนเทศมีอัลกอริทึม (Algorithm) ที่เป็นมาตรฐานเดียวกัน และสามารถตรวจสอบการทำงานได้

นโยบาย

107) ผู้พัฒนาระบบสารสนเทศต้องกำหนดมาตรการป้องกันสภาพแวดล้อมการพัฒนาแบบอย่างมั่นคงปลอดภัยให้ครอบคลุมทั้งวงจรการพัฒนาแบบสารสนเทศ ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

- 107.1 ผู้พัฒนาระบบสารสนเทศควรกำหนดมาตรการป้องกันสภาพแวดล้อมการพัฒนาแบบอย่างมั่นคงปลอดภัยให้ครอบคลุมทั้งวงจรการพัฒนาแบบสารสนเทศ โดยต้องป้องกันข้อมูลของระบบที่เกิดขึ้นในระหว่างการพัฒนา การรับส่งข้อมูล การสำรองข้อมูล และการควบคุมการเข้าถึงระบบสารสนเทศ
- 107.2 หน่วยงานที่จะให้บริการคลาวด์ภายนอกและผู้ใช้ต้องปฏิบัติตามแนวทางปฏิบัติการใช้บริการคลาวด์ พ.ศ. 2566 ซึ่งใช้บังคับอยู่ในปัจจุบัน รวมถึงที่จะได้แก้ไขในอนาคต (ภาคผนวก 9)

นโยบาย

108) เจ้าของระบบสารสนเทศต้องดูแล ควบคุม ติดตามตรวจสอบการทำงานในการจ้างพัฒนาซอฟต์แวร์ ตามระเบียบ คำสั่ง หลักเกณฑ์และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

เจ้าของระบบสารสนเทศควรปฏิบัติดังนี้

- 108.1 กำหนดให้มีการจัดทำสัญญาจ้างการพัฒนาระบบงานโดยให้ครอบคลุมทั้งด้านคุณภาพและความมั่นคงปลอดภัยของระบบงานที่จะมีการพัฒนาขึ้นมาโดยผู้ให้บริการภายนอก
- 108.2 กำหนดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก เช่น การบริหารจัดการโครงการตั้งแต่เริ่มต้นจนกระทั่งแล้วเสร็จ
- 108.3 กำหนดให้มีการระบุว่าจะเป็นผู้มีสิทธิหรือเจ้าของในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดของระบบงานภายใต้โครงการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก
- 108.4 กำหนดให้มีการจัดหาซอฟต์แวร์ที่จะต้องมีการใช้งานภายใต้โครงการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก โดยให้มีจำนวนใบอนุญาตการใช้งานซอฟต์แวร์เหล่านั้นให้ถูกต้องและครบถ้วน
- 108.5 กำหนดให้มีหน่วยงานภายนอกอิสระหรือผู้ที่มีความรู้ความสามารถในการประเมินซอฟต์แวร์ทำหน้าที่ในการรับรองด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่พัฒนาโดยผู้ให้บริการภายนอกนั้น
- 108.8 ตรวจสอบโปรแกรมไม่พึงประสงค์ในซอฟต์แวร์

นโยบาย

109) ผู้พัฒนาระบบสารสนเทศต้องทดสอบด้านความมั่นคงปลอดภัยของระบบที่พัฒนาใหม่หรือระบบงานเดิมที่ปรับปรุง เพื่อให้แน่ใจว่าระบบสารสนเทศสามารถทำงานได้อย่างมั่นคงปลอดภัยตามความต้องการที่กำหนดไว้ โดยให้ปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรส่งระบบที่พัฒนาใหม่หรือระบบงานเดิมที่ปรับปรุงให้หน่วยงานที่เกี่ยวข้องทดสอบด้านความมั่นคงปลอดภัย

นโยบาย

110) หน่วยงานที่เกี่ยวข้องต้องกำหนดให้มีเกณฑ์ในการตรวจรับระบบใหม่ หรือที่ปรับปรุงเพิ่มเติมทั้งที่มาจากการพัฒนาภายในองค์กร หรือที่มีการจัดหาจากจ้างพัฒนา และต้องทดสอบระบบก่อนที่จะนำระบบดังกล่าวมาใช้งานจริง โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

หน่วยงานที่เกี่ยวข้องกับการตรวจรับระบบใหม่ หรือที่ปรับปรุงเพิ่มเติมควรปฏิบัติดังนี้

- 110.1 กำหนดเกณฑ์ในการตรวจรับระบบใหม่ หรือที่ปรับปรุงเพิ่มเติม ทั้งที่มาจากการพัฒนาภายในองค์กร หรือที่มีการจัดหาจากจ้างพัฒนา อย่างเป็นลายลักษณ์อักษร
- 110.2 เกณฑ์การตรวจรับควรมีรายละเอียดดังนี้
 1. มีการทดสอบหรือตรวจสอบมาตรการความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
 2. มีการจัดทำและส่งมอบคู่มือที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ
 3. มีการอบรมบุคลากรที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ
 4. มีการพัฒนาระบบเทคโนโลยีสารสนเทศโดยคำนึงถึงความยากง่ายในการใช้งาน (User Friendliness)
 5. มีการพัฒนาระบบเทคโนโลยีสารสนเทศโดยคำนึงถึงการป้องกันความผิดพลาดโดยมนุษย์ในการใช้งานระบบ (Human Errors)
 6. มีการระบุข้อกำหนดด้านความต้องการในการกู้คืนระบบเทคโนโลยีสารสนเทศ
- 110.3 ทดสอบระบบก่อนที่จะนำระบบดังกล่าวมาใช้งานจริง

นโยบาย

111) การนำข้อมูลมาใช้ทดสอบในระบบสารสนเทศ ให้ผู้พัฒนาระบบสารสนเทศเลือกข้อมูลมาใช้งานอย่างระมัดระวัง โดยให้มีการป้องกัน ควบคุม เพื่อไม่ให้ข้อมูลสำคัญรั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต ตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรปฏิบัติดังนี้

- 111.1 ไม่อนุญาตการใช้ข้อมูลส่วนบุคคลหรือข้อมูลสำคัญเพื่อใช้ในการทดสอบกับระบบงาน
- 111.2 กำหนดให้มีการลบข้อมูลส่วนที่ บังคับตัวบุคคลทิ้งไปก่อนนำข้อมูลนั้นไปใช้ในการทดสอบกับระบบงาน เช่น ลบชื่อนามสกุลทิ้งไป เป็นต้น
- 111.3 กำหนดให้มีการลบข้อมูลส่วนที่มีความสำคัญทิ้งไปก่อนนำข้อมูลนั้นไปใช้ในการทดสอบกับระบบงาน เช่น ข้อมูลเงินเดือน เป็นต้น
- 111.4 กำหนดให้มีการขออนุมัติก่อนทุกครั้งก่อนที่จะนำข้อมูลบนเครื่องให้บริการไปใช้ในการทดสอบกับระบบงาน
- 111.5 กำหนดให้ทำการลบข้อมูลจริงซึ่งนำไปใช้ในการทดสอบโดยทันทีหลังจากที่ใช้งานเสร็จ

นโยบาย

112) ผู้พัฒนาระบบสารสนเทศต้องตรวจสอบ (Validate) ข้อมูลใด ๆ ก่อนที่จะรับเข้าสู่แอปพลิเคชันเสมอ เพื่อให้มั่นใจได้ว่าข้อมูลมีความถูกต้องและมีรูปแบบเหมาะสม โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟผ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรปฏิบัติดังนี้

- 112.1 กำหนดให้มีการตรวจสอบข้อมูลนำเข้าสู่ระบบงาน (แอปพลิเคชัน) เพื่อให้ข้อมูลนั้นมีความถูกต้องและเหมาะสมก่อนนำไปใช้ในการประมวลผล
- 112.2 กำหนดให้มีการตรวจสอบข้อมูลนำเข้าสู่ระบบงาน (แอปพลิเคชัน) ดังนี้
 1. ข้อมูลนำเข้าควรตรงกับชนิดของข้อมูลที่ต้องการ
 2. ข้อมูลนำเข้าควรอยู่ภายในช่วงของค่าที่ต้องการ
 3. ข้อมูลนำเข้าควรอยู่ภายในค่าขอบเขตบนและล่างที่ต้องการ
 4. ข้อมูลนำเข้าควรมีความครบถ้วน
 5. ข้อมูลนำเข้าไม่ควรมีตัวอักษรหรืออักขระพิเศษต่าง ๆ ที่นอกเหนือจากที่ต้องการ
 6. ระบบงาน (แอปพลิเคชัน) ต้องระบุว่าข้อมูลที่นำเข้าไม่ได้ Error เพราะอะไร)
- 112.3 กำหนดให้มีการตรวจสอบฟิลด์ หรือไฟล์ข้อมูลที่สำคัญๆ อย่างสม่ำเสมอ เพื่อตรวจสอบความถูกต้องและเหมาะสมของข้อมูลเหล่านั้น
- 112.4 กำหนดให้มีการตรวจสอบจากเอกสารที่จะใช้เป็นข้อมูลนำเข้า เพื่อตรวจหาการเปลี่ยนแปลงที่เกิดขึ้นโดยไม่ได้รับอนุญาต เช่น มีการขีดฆ่าหรือลบโดยไม่มีลายมือชื่อกำกับ เป็นต้น
- 112.5 กำหนดขั้นตอนปฏิบัติสำหรับการจัดการกับข้อผิดพลาดที่ตรวจพบในข้อมูลนำเข้า
- 112.6 กำหนดบุคลากรที่ทำหน้าที่ในการนำข้อมูลเข้าสู่ระบบงาน รวมทั้งกำหนดบทบาทและหน้าที่ความรับผิดชอบ
- 112.7 กำหนดให้มีการบันทึกล็อกสำหรับกิจกรรมการนำข้อมูลเข้าสู่ระบบงาน

นโยบาย

113) ผู้รับผิดชอบสารสนเทศต้องตรวจสอบ (Validate) การทำงานของแอปพลิเคชันเพื่อตรวจหาข้อผิดพลาดของข้อมูลที่อาจเกิดจากการทำงานหรือการประมวลผลที่ผิดพลาด โดยถือปฏิบัติตามระเบียบคำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

- 113.1 ออกแบบระบบงาน (แอปพลิเคชัน) เพื่อช่วยลดความเสี่ยงในการประมวลผลผิดพลาด เช่น การออกแบบหน้าจอสำหรับรับข้อมูลนำเข้าที่เหมาะสม สามารถช่วยลดความผิดพลาดในการประมวลผลข้อมูลได้ เป็นต้น
- 113.2 กำหนดขั้นตอนปฏิบัติเพื่อป้องกันระบบงาน (แอปพลิเคชัน) ทำงานต่อไปหลังจากที่เกิดข้อผิดพลาดขึ้น
- 113.3 กำหนดขั้นตอนปฏิบัติเพื่อป้องกันระบบงานทำงานผิดพลาดหลังจากที่เกิดข้อผิดพลาดขึ้น
- 113.4 กำหนดให้มีการออกแบบระบบงานเพื่อป้องกันปัญหาหน่วยความจำล้น (Buffer Overflows) เช่น การนับจำนวนตัวอักษรหรืออักขระที่รับเข้ามาเพื่อไม่ให้เกินจำนวนตามที่ต้องการ เป็นต้น

- 113.5 กำหนดให้มีมาตรการเพื่อแก้ไขและกักเก็บคืนไปสู่จุดที่มีการประมวลผลผิดพลาด หรือที่ฐานข้อมูลของระบบงานเกิดความเสียหาย (เช่น ฮาร์ดดิสก์เกิดความเสียหาย) เพื่อให้ระบบงานสามารถประมวลผลต่อไปได้อย่างต่อเนื่องและถูกต้อง
- 113.6 กำหนดให้มีการตรวจหาข้อผิดพลาดที่เกิดขึ้นจากการประมวลผล เช่น
1. การตรวจสอบความถูกต้องของผลการประมวลผลแบบกลุ่ม (Batch Processing) เช่น การตรวจนับด้วยมือเมื่อเทียบกับผลการประมวลผลด้วยระบบงาน
 2. การตรวจสอบยอดที่ยกมาโดยเทียบกับยอดที่ปิดไปก่อนหน้านี้ (โดยปกติในทางบัญชียอดที่ยกมาควรเท่ากับยอดที่ปิดไปก่อนหน้านี้)
 3. การคำนวณค่าผลรวมเพื่อดูว่ามีบางรายการเกิดการสูญหาย ไม่ครบถ้วนหรือไม่ เช่น คำนวณด้วยตนเองในฟิลด์หมายเลขเช็คโดยนำหมายเลขเช็คบวกเข้าด้วยกันทั้งหมด ซึ่งจะได้ค่าผลรวมออกมาเป็นค่าหนึ่ง และนำค่านี้ไปเปรียบเทียบกับค่าผลรวมที่คำนวณด้วยระบบงานสำหรับฟิลด์เดียวกัน
 4. การตรวจสอบข้อมูลล็อกซึ่งแสดงถึงกิจกรรมการประมวลผลที่เกิดขึ้น
 5. การทำงานของระบบงานว่าตรงตามกำหนดการที่วางไว้หรือไม่
 6. การตรวจสอบลำดับการประมวลผลของระบบงานว่าทำงานตามลำดับที่ต้องการหรือไม่
 7. การตรวจสอบว่ามีการสิ้นสุดการทำงานของระบบงานอย่างกะทันหันเกิดขึ้นหรือไม่ (ซึ่งอาจแสดงถึงการทำงานที่ผิดพลาดของระบบงาน)

นโยบาย

114) ผู้พัฒนาระบบสารสนเทศต้องรักษาความถูกต้องแท้จริง (Authenticity) และความถูกต้องครบถ้วน (Integrity) ของข้อมูลในแอปพลิเคชัน เพื่อป้องกันและสร้างความมั่นใจว่าข้อมูลที่ได้รับจากการรับ-ส่งข้อมูลเป็นข้อมูลที่ถูกต้องแท้จริง มาจากผู้ส่งที่ถูกต้อง และไม่ถูกแก้ไขระหว่างทางหรือถูกแก้ไขโดยผู้ไม่มีสิทธิ โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้พัฒนาระบบสารสนเทศควรปฏิบัติดังนี้

- 114.1 ตรวจสอบว่าผู้ส่งข้อมูลมาคือใคร ถ้าตรวจสอบแล้วว่าเป็นผู้ส่งข้อมูลที่ต้องการ ก็จะมี ความถูกต้องแท้จริง (Authenticity)
- 114.2 ตรวจสอบข้อมูลที่ส่งมามีความถูกต้องครบถ้วน (Integrity) เช่นเดียวกับข้อมูลจากต้นทางหรือไม่

นโยบาย

115) ผู้รับผิดชอบสารสนเทศและผู้ใช้ต้องร่วมกันดำเนินการให้มีการตรวจสอบ (Validate) ข้อมูลใด ๆ อันเป็นผลจากการประมวลผลของแอปพลิเคชัน เพื่อให้มั่นใจได้ว่าข้อมูลที่ได้จากการประมวลผลถูกต้องและเหมาะสม โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของ กพท. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

- 115.1 ตรวจสอบข้อมูลที่น่าออกจากระบบงาน (แอปพลิเคชัน) เพื่อตรวจสอบความถูกต้อง ความเหมาะสม ความสมบูรณ์ และความสมเหตุสมผล ก่อนนำไปใช้งาน หรือใช้ประโยชน์ต่อไป
- 115.2 กำหนดให้ผู้รับผิดชอบสำหรับการตรวจสอบข้อมูลที่น่าออกจากระบบงาน
- 115.3 กำหนดให้มีการตรวจสอบข้อมูลนำเข้าระบบงาน (ข้อมูลนั้นนำมาจากอีกระบบงานหนึ่ง) เพื่อให้ข้อมูลมีความถูกต้อง เหมาะสม และสมบูรณ์ ก่อนที่จะนำข้อมูลนั้นเข้าสู่กระบวนการประมวลผลต่อไป
- 115.4 จัดทำขั้นตอนปฏิบัติเพื่อจัดการกับข้อผิดพลาดที่พบในข้อมูลที่น่าออกจากระบบงาน
- 115.5 กำหนดให้มีการนับจำนวนรายการข้อมูลในระบบงานนั้นเทียบกับรายการข้อมูลที่น่าเข้าไปประมวลผลว่าตรงกันหรือไม่ เช่น ขนาดข้อมูล จำนวนฟิลด์ จำนวน Record
- 115.6 กำหนดให้มีการบันทึกข้อมูลสื่อแสดงกิจกรรมการตรวจสอบข้อมูลที่น่าออกจากระบบงาน

นโยบาย

116) ผู้รับผิดชอบสารสนเทศต้องป้องกันการรั่วไหลของข้อมูลสารสนเทศ โดยถือปฏิบัติตามระเบียบ คำสั่ง หลักเกณฑ์ และหรือแนวทางปฏิบัติที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศของ กฟภ. ที่ประกาศใช้ในปัจจุบัน

แนวทางปฏิบัติ

ผู้รับผิดชอบสารสนเทศควรปฏิบัติดังนี้

- 116.1 ป้องกันโปรแกรมไม่พึงประสงค์ประเภทม้าโทรจัน (Trojan Horses) ซึ่งเมื่อถูกติดตั้งลงไปในระบบเทคโนโลยีสารสนเทศของ กฟภ. แล้ว อาจแอบขโมยและส่งข้อมูลของ กฟภ. ไปให้แก่ผู้ไม่ประสงค์ดี
- 116.2 ตรวจสอบสื่อบันทึกข้อมูลและระบบสื่อสารข้อมูลอย่างสม่ำเสมอเพื่อป้องกันการแอบส่งข้อมูลผ่านทางสื่อบันทึกข้อมูลหรือระบบสื่อสารข้อมูลนั้น
- 116.3 เข้ารหัสข้อมูลเพื่อซ่อนข้อมูลที่มีการรับ-ส่ง
- 116.4 ใช้ซอฟต์แวร์หรือระบบงานที่ได้รับการตรวจสอบแล้วว่ามีการทำงานที่ถูกต้อง และเชื่อถือได้ หรือใช้ซอฟต์แวร์ที่ได้รับการประเมินและรับรองแล้ว เช่น ตามมาตรฐาน ISO/IEC 15408 เป็นต้น
- 116.5 เฝ้าระวังและตรวจสอบกิจกรรมของผู้ใช้ในระบบงานอย่างสม่ำเสมอ แต่ต้องระมัดระวังไม่ให้ขัดแย้งกับกฎหมายหรือข้อกำหนดที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการละเมิดสิทธิส่วนบุคคล เป็นต้น
- 116.6 เฝ้าระวังและตรวจสอบการใช้ทรัพยากรสารสนเทศของ กฟภ. อย่างสม่ำเสมอ เพื่อป้องกันการใช้ผิดวัตถุประสงค์