การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

แนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ
ประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. ๒๕๖๒

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

การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

ประกาศการไฟฟ้าส่วนภูมิภาค

เรื่อง มาตรการการใช้ทรัพย์สินสารสนเทศ ของ กฟภ.

พ.ศ. ๒๕๖๓

.....

การไฟฟ้าส่วนภูมิภาค เป็นองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ เพื่อเป็นการป้องกันภัยคุกคามที่อาจเกิดขึ้นกับระบบสารสนเทศของ กฟภ. รวมทั้งเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพย์สินสารสนเทศ ของ กฟภ. จึงเห็นสมควรกำหนดมาตรการการใช้ทรัพย์สินสารสนเทศ ของ กฟภ. ให้พนักงานและลูกจ้าง ทราบและถือปฏิบัติในระดับเคร่งครัด ดังนี้

๑) ห้ามดาวน์โหลดและติดตั้งซอฟต์แวร์นอกเหนือจากที่ กฟภ. จัดหาให้

๒) ห้ามติดตั้งและเชื่อมต่อเครือข่ายภายนอก เช่น 4G/ADSL หรืออื่นๆ โดยเด็ดขาด เว้นแต่เครือข่ายภายนอกที่ได้รับอนุมัติให้ติดตั้ง

๓) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัว เชื่อมต่อเข้าระบบเครือข่ายของ กฟภ. หากมีความจำเป็น ต้องปฏิบัติตามหลักเกณฑ์การใช้งานของ กฟภ.

๔) ให้เก็บรักษา ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนเองไว้เป็นความลับ

๕) ให้ติดตั้ง Anti-Virus หรือ ซอฟต์แวร์ที่เกี่ยวข้องกันการรักษาความมั่นคงปลอดภัย ตามที่ กฟภ. กำหนด

๖) ให้ใช้ระบบปฏิบัติการ และซอฟต์แวร์ที่มีลิขสิทธิ์ (License) ถูกต้อง

๗) ให้เข้าถึงเฉพาะบริการทางเครือข่ายตามสิทธิที่ได้รับอนุญาตให้ใช้ได้เท่านั้น

๘) ให้ใช้ทรัพย์สินสารสนเทศเพื่อปฏิบัติงานของ กฟภ. เท่านั้น

๙) ให้สำรองข้อมูลที่สำคัญอย่างสม่ำเสมอ โดยใช้เครื่องมือและวิธีการที่ กฟภ. กำหนด

๑๐) ให้ใช้ Email ของ กฟภ. ในการทำงานเท่านั้น และห้ามนำไปใช้กิจส่วนตัว

ทั้งนี้ หากพนักงานและลูกจ้างของ กฟภ. ฝ่าฝืนไม่ปฏิบัติตามมาตรการฯ ดังกล่าวข้างต้น ผู้รับผิดชอบสารสนเทศจะระงับสิทธิของผู้ใช้ และหากการฝ่าฝืนดังกล่าวก่อให้เกิดความเสียหายแก่ กฟภ. หรือบุคคลอื่น ให้ดำเนินการตั้งคณะกรรมการสอบสวนทางวินัย และหรือความรับผิดทางละเมิดตามข้อบังคับและระเบียบ ของ กฟภ.

ประกาศ ณ วันที่ - 6 สค. 2563

(นายสมพงษ์ ปรีเปรม)
ผู้ว่าการการไฟฟ้าส่วนภูมิภาค

กองอำนวยการ
เลขที่ ๒๒๔
วันที่ ๑๑ มิ.ย. ๒๕๖๔
เวลา ๑๐.๒๔ น.

การไฟฟ้าส่วนภูมิภาค
PROVINCIAL ELECTRICITY AUTHORITY

จาก ฝกง. ถึง ทุกหน่วยงาน

เลขที่ ฝกง. 151/2564 วันที่ 11 มิ.ย. 2564

เรื่อง แจ้งเวียนแนวทางปฏิบัติในการใช้ การป้องกัน และการรักษา (Password) ของพนักงานและลูกจ้างผู้รับผิดชอบที่เกี่ยวข้องกับระบบการเงิน

เรียน รผก., ผชก., อส., ผชช., อฝ., อก. และ ผจก.กฟฟ. ทุกแห่ง

ฝกง. ขอแจ้งเวียนแนวทางปฏิบัติในการใช้ การป้องกัน และการรักษา (Password) ของพนักงานและลูกจ้าง ผู้รับผิดชอบที่เกี่ยวข้องกับระบบการเงิน เพื่อรักษาความมั่นคงปลอดภัยของระบบการเงิน ดังนี้

1. ผู้บังคับบัญชาขั้นต้นขึ้นไป ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงเฉพาะระบบการเงินที่ได้รับอนุญาตให้ใช้ได้เท่านั้น โดยสิทธิที่ได้รับต้องเป็นไปตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน ทั้งนี้ เมื่อพนักงานและลูกจ้างผู้รับผิดชอบที่เกี่ยวข้องกับระบบการเงินได้รับแจ้งยุติการจ้าง หรือการเปลี่ยนแปลงสภาพการจ้าง โยกย้ายหน่วยงาน การพักงาน ระงับการปฏิบัติหน้าที่ การปรับเปลี่ยนบุคลากร หรือการสิ้นสุดสัญญาจ้าง ผู้บังคับบัญชาต้องยกเลิกหรือเปลี่ยนแปลงสิทธิในการเข้าใช้งานระบบทางการเงินนั้นทันที

2. พนักงานและลูกจ้าง ควรกำหนดรหัสผ่านในการเข้าถึงระบบการเงิน ดังนี้

2.1 ตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำของตนเอง และเป็นรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

2.2 หลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยตัวอักขระที่เรียงกัน กลุ่มของตัวอักขระที่เหมือนกัน

2.3 เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผย

2.4 รหัสผ่านอาจผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวอักขระพิเศษ และสัญลักษณ์ต่างๆ

2.5 เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับครั้งแรกทันทีที่ทำการล็อกอินเข้าสู่ระบบงาน

2.6 ไม่กำหนดรหัสผ่านจากชื่อ ชื่อสกุลของผู้ใช้ ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตน คำศัพท์ที่ใช้ในพจนานุกรม หมายเลขโทรศัพท์

2.7 เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

2.8 ผู้ใช้ควรทำการเปลี่ยนรหัสผ่านทุกๆ 6 เดือน

2.9 ไม่กำหนดให้ระบบงานทำการบันทึกรหัสผ่านที่ใช้งาน

2.10 ไม่ใช้รหัสผ่านของตนร่วมกับผู้อื่น และเปิดเผยรหัสผ่านของตนแก่ผู้อื่น

2.11 เก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย และต้องไม่บันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่นๆ

โดยให้ถือปฏิบัติตามแนวทางปฏิบัติความมั่นคงปลอดภัยสารสนเทศ ประกอบนโยบายความมั่นคงปลอดภัยสารสนเทศ พ.ศ. 2562 หมวด 5 การควบคุมการเข้าถึง (ตามเอกสารแนบ 1) และตามประกาศการไฟฟ้าส่วนภูมิภาค เรื่องมาตรการการใช้ทรัพย์สินสารสนเทศของ กฟภ. พ.ศ. 2563 (ตามเอกสารแนบ 2)

จึงเรียนมาเพื่อโปรดทราบ และแจ้งพนักงาน ลูกจ้างที่เกี่ยวข้องถือปฏิบัติ ต่อไปด้วยจะขอบคุณยิ่ง

เรียน รก.นก.(๐)
เพื่อดำเนินการต่อไปด้วย

(นางสาวจุฑารัตน์ ชูวาพิทักษ์)
อฝ.กง.

(นายพันเลิศ บุญประสงค์)
รก.นก. รักษาการแทน อก.นก.
๑๑ มิ.ย. ๒๕๖๔

ผวพ.กกง.
โทร. 9985
D:\Jirati\Documents\รักษา Password