คำสั่งสำนักงานคณะกรรมการกำกับกิจการพลังงาน

ที่ ๐๗๕ /๒๕๕๖

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักงานคณะกรรมการกำกับกิจการพลังงาน พ.ศ. ๒๕๕๖

ตามที่ สำนักงานคณะกรรมการกำกับกิจการพลังงาน (สำนักงาน กกพ.) ได้นำเทคโนโลยีสารสนเทศมาเพิ่มประสิทธิภาพการทำงานในด้านต่างๆ ทั้งด้านสนับสนุนการให้บริการผู้มีส่วนได้เสียกลุ่มต่างๆ และการปฏิบัติงานภายใน ทั้งนี้เทคโนโลยีสารสนเทศมีการเชื่อมโยงกันทั้งภายในและภายนอกสำนักงาน กกพ. รวมทั้งเกี่ยวข้องกับข้อมูลสารสนเทศต่างๆ มากมาย จึงมีความเสี่ยงต่อการโจมตี (Intrusion) จากผู้ไม่ประสงค์ดีหรือเกิดความเสี่ยงต่อการสูญหายของข้อมูลสารสนเทศที่สำคัญ อันเนื่องมาจากเหตุร้ายต่างๆ หรือจากการนำข้อมูลไปใช้โดยไม่ถูกต้อง ทำให้สำนักงาน กกพ. ได้รับความเสียหาย

ดังนั้น เพื่อให้การบริการและการสนับสนุนการปฏิบัติงานของสำนักงาน กกพ. ได้รับการยอมรับเชื่อถือและเป็นที่ไว้วางใจจากผู้มีส่วนได้เสียกลุ่มต่างๆ และผู้ปฏิบัติงานภายใน รวมทั้งเพื่อความมั่นคงปลอดภัยจากการบุกรุก ทำลายจากผู้ไม่ประสงค์ดี สำนักงาน กกพ. จึงกำหนดให้มี “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานคณะกรรมการกำกับกิจการพลังงาน พ.ศ. ๒๕๕๖” ขึ้นตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการ ทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ โดยอ้างอิงมาตรฐาน ISO ๒๗๐๐๑ ทั้งนี้ให้ทุกหน่วยงานและพนักงานของสำนักงาน กกพ. ถือปฏิบัติในส่วนที่เกี่ยวข้องตามนโยบายฯ ฉบับดังกล่าว ที่แนบท้ายคำสั่งฉบับนี้อย่างเคร่งครัด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑๗ เมษายน พ.ศ. ๒๕๕๖

(นายกวิน ทังสุพานิช)

เลขาธิการสำนักงานคณะกรรมการกำกับกิจการพลังงาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานคณะกรรมการกำกับกิจการพลังงาน
พ.ศ. ๒๕๕๖

คำนำ

ตามที่ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๗ กำหนดให้หน่วยงานของภาครัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่างๆของหน่วยงานรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

ดังนั้น สำนักงานคณะกรรมการกำกับกิจการพลังงาน จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการกำกับกิจการพลังงาน พ.ศ. ๒๕๕๖ เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฯจากบุคลากรทุกคน และต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว สำนักงานคณะกรรมการกำกับกิจการพลังงาน จึงหวังเป็นอย่างยิ่งว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของสำนักงานคณะกรรมการกำกับกิจการพลังงานทุกคน ถือปฏิบัติโดยเคร่งครัดต่อไป

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานคณะกรรมการกำกับกิจการพลังงาน พ.ศ. ๒๕๕๖

หลักการและเหตุผล

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ ดังนั้น สำนักงานคณะกรรมการกำกับกิจการพลังงาน จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องได้นำไปปฏิบัติอย่างเคร่งครัด

วัตถุประสงค์

๑ เพื่อให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการกำกับกิจการพลังงานเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒ เพื่อกำหนดแนวทางและวิธีการปฏิบัติสำหรับบุคลากรและบุคคลที่ปฏิบัติงานให้กับสำนักงานคณะกรรมการกำกับกิจการพลังงาน ในการยืนยันตัวบุคคล การเข้าถึงและการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

๓ เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีแผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ตามปกติ ให้มีระบบสำรองสามารถทำงานได้อย่างต่อเนื่องและสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๔ เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๕ เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ ความเข้าใจและการให้การอบรมทางด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้แก่บุคลากรและบุคคลที่เกี่ยวข้อง

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานคณะกรรมการกำกับกิจการพลังงาน พ.ศ. ๒๕๕๖

๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของสำนักงานคณะกรรมการกำกับกิจการพลังงาน

๒ มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายที่เกี่ยวข้อง

๓ เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๔ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรของสำนักงานคณะกรรมการกำกับกิจการพลังงานและบุคคลที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

๕ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานคณะกรรมการกำกับกิจการพลังงาน พ.ศ. ๒๕๕๖

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานคณะกรรมการกำกับกิจการพลังงานจัดทำขึ้นเพื่อกำหนดวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยแบ่งนโยบายออกเป็นส่วนๆ ดังต่อไปนี้

ส่วนที่ ๑. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
ส่วนที่ ๒. แนวปฏิบัติการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย
ส่วนที่ ๓. แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย
ส่วนที่ ๔. แนวปฏิบัติของผู้ดูแลระบบ
ส่วนที่ ๕. แนวปฏิบัติการจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน
ส่วนที่ ๖. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง
ส่วนที่ ๗. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
ส่วนที่ ๘. การกำหนดผู้รับผิดชอบ

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

“สำนักงาน” หมายถึง สำนักงานคณะกรรมการกำกับกิจการพลังงาน (สำนักงาน กกพ.)

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย” หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของสำนักงานคณะกรรมการกำกับกิจการพลังงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

“ความมั่นคงปลอดภัย” หมายถึง ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการกำกับกิจการพลังงาน

“ระบบแลน (Local Area Network)” และ **“ระบบอินทราเน็ต (Intranet)”** หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในสำนักงานคณะกรรมการกำกับกิจการพลังงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในสำนักงานคณะกรรมการกำกับกิจการพลังงาน

“ระบบอินเทอร์เน็ต (Internet)” หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของสำนักงานคณะกรรมการกำกับกิจการพลังงาน เข้ากับเครือข่ายอินเทอร์เน็ตสากล

“ระบบเทคโนโลยีสารสนเทศ (Information Technology System)” หมายถึง ระบบงานของสำนักงานคณะกรรมการกำกับกิจการพลังงาน ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สำนักงานคณะกรรมการกำกับกิจการพลังงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

“เครื่องคอมพิวเตอร์” หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“สารสนเทศ (Information)” หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

“ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงาน กกพ.

“ผู้ใช้งาน” หมายถึง คณะกรรมการกำกับกิจการพลังงาน พนักงานหรือลูกจ้างของสำนักงานคณะกรรมการกำกับกิจการพลังงาน รวมถึงบุคคลภายนอกที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของสำนักงานคณะกรรมการกำกับกิจการพลังงาน

“ผู้ดูแลระบบ (System Administrator)” หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“บุคคลภายนอก” หมายถึง บุคคลที่ไม่ได้สังกัดอยู่ในสำนักงานคณะกรรมการกำกับกิจการพลังงาน แต่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่างๆ ของสำนักงานคณะกรรมการกำกับกิจการพลังงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร” หมายถึง พื้นที่ที่สำนักงานคณะกรรมการกำกับกิจการพลังงาน อนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

(๑) ที่ทำงาน หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลประจำโต๊ะทำงาน และคอมพิวเตอร์แบบพกพา รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ (System Administrator)

(๒) พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่ายหมายถึง บริเวณติดตั้งเครื่อง Server และอุปกรณ์เครือข่ายทั้งของสำนักงานกลาง และสำนักงานประจำเขต

(๓) พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายถึง พื้นที่ครอบคลุมในการให้บริการระบบเครือข่ายไร้สาย

“สินทรัพย์” หมายถึง ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการกำกับกิจการพลังงาน เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

“จดหมายอิเล็กทรอนิกส์ (e-mail)” หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

“รหัสผ่าน (Password)” หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“บัญชีผู้ใช้งาน (Account)” หมายถึง รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของสำนักงานคณะกรรมการกำกับกิจการพลังงาน

“เวลาอ้างอิงสากล (Stratum 0)” หมายถึง การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล ในประเทศไทยนั้นเราอ้างอิงกับหน่วยงานมาตรฐาน (เช่น กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ) เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

“ข้อมูลจราจรทางคอมพิวเตอร์ (Log)” หมายถึง ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่นๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“โปรแกรมประสงค์ร้าย (Malware)” หมายถึง โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

“ชื่อเครื่องคอมพิวเตอร์ (Computer Name)” หมายถึง ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

“สื่อบันทึกพกพา” หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

“ปุ่มกดง่าย (Shortcut)” หมายถึง เครื่องมือที่ช่วยในการเรียกใช้โปรแกรมได้อย่างรวดเร็วและสามารถเข้าถึงโปรแกรมหรือแฟ้มข้อมูลที่ต้องการได้ทันที ซึ่งผู้ใช้สามารถลบหรือสร้างใหม่ได้

“ไบออส (BIOS)” หมายถึง ซอฟต์แวร์ขนาดเล็กซึ่งเก็บอยู่ในหน่วยความจำบนเมนบอร์ดของเครื่องคอมพิวเตอร์ ทำหน้าที่ควบคุมขั้นตอนการบู๊ตและการทำงานของอุปกรณ์พื้นฐานต่างๆ ที่ติดตั้งอยู่บนเมนบอร์ด

“การตั้งค่าระบบ (Configuration)” หมายถึง ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

“เลขที่อยู่ไอพี (IP Address)” หมายถึง ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

“เลขที่อยู่ไอพีสาธารณะ (Public IP Address)” หมายถึง เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงาน หรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

“แบนด์วิดท์ (Bandwidth)” หมายถึง ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

“ชื่อผู้ใช้ (Username)” หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

“ลงบันทึกเข้า (Login)” หมายถึง กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

“ลงบันทึกออก (Logout)” หมายถึง กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

“อัพเดท (Update)” หมายถึง ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

“ช่องโหว่ (Vulnerability)” หมายถึง ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

“ไฟล์ที่สามารถประมวลผลได้ (Executable file)” หมายถึง ไฟล์โปรแกรมที่สามารถเรียกใช้งานได้ทันที เช่น .exe .com .bat .vbs .scr .pif .hta .txt .doc .xls ในขณะที่ไฟล์ข้อมูลอื่นๆ จะเป็นไฟล์ข้อมูลประกอบ

“การเข้ารหัส (Encryption)” หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

“อุปกรณ์กระจายสัญญาณ (Access Point)” หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

“SSID (Service Set Identifier)” หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

“โดยปริยาย (Default)” หมายถึง ค่าที่เครื่องคอมพิวเตอร์หรือโปรแกรมได้กำหนดไว้ล่วงหน้า และนำไปใช้ได้โดยปริยายหากไม่มีการเปลี่ยนแปลงจากผู้ใช้งาน

“WEP (Wired Equivalent Privacy)” หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

“WPA (Wi-Fi Protected Access)” หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

“Wireless LAN Client” หมายถึง เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลน โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ โดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ ซึ่งมีมาตรฐานที่นิยมใช้เรียกว่า IEEE 802.11

“MAC Address (Media Access Control Address)” หมายถึง หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

“ไฟร์วอลล์ (Firewall)” หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

“VPN (Virtual Private Network)” หมายถึง เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

“Web Server” หมายถึง เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บ และมีหน้าที่ให้บริการเว็บเพจต่างๆ

“ชื่อโดเมนย่อย (Sub Domain Name)” หมายถึง ส่วนย่อยที่จะช่วยขยายให้ทราบถึงกลุ่มต่าง ๆ ภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ “ที่อยู่เว็บไซต์” แทนก็ได้

“อุปกรณ์จัดเส้นทาง (Router)” หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

“อุปกรณ์กระจายสัญญาณข้อมูล (Switch)” หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล

“การพิสูจน์ยืนยันตัวตน (Authentication)” หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยว ข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

“แผนผังระบบเครือข่าย (Network Diagram)” หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของสำนักงานคณะกรรมการกำกับกิจการพลังงาน

“Command Line” หมายถึง บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความ เพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ

“Firewall Log” หมายถึง การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟร์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์ เพื่อตรวจสอบประเภทของการสื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในสำนักงานคณะกรรมการกำกับกิจการพลังงาน

“DOD 5220.22-M” หมายถึง การลบข้อมูลอย่างสมบูรณ์ซึ่งได้รับการยอมรับและใช้งานกับกระทรวงกลาโหม ประเทศสหรัฐอเมริกา โดยทำให้ไม่สามารถกู้ไฟล์กลับคืนมาได้ ซึ่งทำการลบข้อมูล ๓ รอบรอบแรกด้วยข้อมูลแบบสุ่ม รอบที่สองด้วยบิตที่ตรงกันข้าม รอบสุดท้ายด้วยข้อมูลไบต์สุ่ม

“ผู้ตรวจสอบระบบสารสนเทศของสำนักงานคณะกรรมการกำกับกิจการพลังงาน (Internal IT Auditor)” หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่ตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Log) และรับผิดชอบให้สามารถเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ (Log)

“ผู้ตรวจสอบระบบสารสนเทศจากหน่วยงานภายนอก (External IT Auditor)” หมายถึง ผู้ที่ได้รับมอบหมายจากสำนักงานคณะกรรมการกำกับกิจการพลังงาน ให้มีสิทธิในการตรวจสอบระบบสารสนเทศหรือระบบเครือข่ายของสำนักงานคณะกรรมการกำกับกิจการพลังงาน

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“ความมั่นคงปลอดภัย” หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน(Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และ ความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย (Information security event)” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือระบบเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident)” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจไม่คาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ส่วนที่ ๑

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานที่เป็นบุคลากรของสำนักงาน และบุคคลภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน

๒. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๑ ให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้งาน พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๒.๒ ให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓ ให้ฝ่ายเทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๒.๔ บุคคลภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในสำนักงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

ส่วนที่ ๒

แนวปฏิบัติการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย

๑. วัตถุประสงค์

เพื่อช่วยให้ผู้ใช้งานที่เป็นบุคลากรของสำนักงานและบุคคลภายนอก ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของสำนักงาน ให้เป็นความลับ มีความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒.๑ ผู้ใช้งานจะต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายโดยมีวัตถุประสงค์ ดังต่อไปนี้

๒.๑.๑ ทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนสู่ระบบคอมพิวเตอร์

๒.๑.๒ นำข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นเข้าสู่ระบบคอมพิวเตอร์

๒.๑.๓ นำข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชนเข้าสู่ระบบคอมพิวเตอร์

๒.๑.๔ นำข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญาเข้าสู่ระบบคอมพิวเตอร์

๒.๑.๕ นำข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้เข้าสู่ระบบคอมพิวเตอร์

๒.๑.๖ นำข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย เข้าสู่ระบบคอมพิวเตอร์

๒.๑.๗ เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม ๒.๑.๑ ถึง ๒.๑.๖

๒.๒ ผู้ใช้งานจะต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตาม ๒.๑ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

๒.๓ ผู้ใช้งานจะต้องไม่กระทำการ ดังต่อไปนี้

๒.๓.๑ เข้าใช้ระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตนโดยมิชอบ

๒.๓.๒ นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ เช่น รหัสผ่าน ไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

๒.๓.๓ เข้าถึงซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนโดยมิชอบ

๒.๓.๔ กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

๒.๓.๕ ทำให้ข้อมูลคอมพิวเตอร์ของผู้อื่นเสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน โดยมิชอบ

๒.๓.๖ กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานได้ตามปกติ

๒.๓.๗ ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-mail) แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่น

๒.๓.๘ กระทำให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

๒.๓.๙ สำนักงานเป็นผู้มีหน้าที่จัดคอมพิวเตอร์แบบตั้งโต๊ะและพกพา พร้อมโปรแกรมคอมพิวเตอร์ที่จำเป็นต่อการใช้งานและถูกต้องตามกฎหมาย หากบุคคลใดมีความประสงค์ต้องการใช้งานโปรแกรมคอมพิวเตอร์อื่นนอกเหนือจากที่ทางสำนักงานจัดไว้ ให้แจ้งความประสงค์มายังฝ่ายเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรเพื่อพิจารณาจัดหาต่อไป

๒.๓.๑๐ จำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม ๒.๓.๑ ถึง ๒.๓.๘

๒.๓.๑๑ ผู้ใช้งานจะต้องรับผิดชอบลิขสิทธิ์โปรแกรมคอมพิวเตอร์และการกระทำใดๆ อันเกิดจากการใช้คอมพิวเตอร์แบบพกพา (Notebook) อันเป็นทรัพย์สินส่วนตัวของผู้ใช้งาน

๒.๓.๑๒ ห้ามมิให้ผู้ใช้งานทำการแก้ไขเปลี่ยนแปลงการตั้งค่าพารามิเตอร์ต่างๆของคอมพิวเตอร์ เช่น Computer Name, System Configuration และ Program Configuration เว้นแต่เป็นผู้มีหน้าที่ดูแลระบบคอมพิวเตอร์หรือ ระบบเครือข่ายคอมพิวเตอร์

๒.๓.๑๓ ห้ามมิให้ผู้ใช้ติดตั้งโปรแกรมคอมพิวเตอร์ด้วยตนเอง เว้นแต่เป็นผู้มีหน้าที่ดูแลระบบคอมพิวเตอร์ หรือ ระบบเครือข่ายคอมพิวเตอร์

๒.๓.๑๔ ห้ามมิให้ใช้ระบบคอมพิวเตอร์และเครือข่ายของสำนักงาน เพื่อการพาณิชย์หรือการอื่นใดที่ไม่เกี่ยวข้องกับหน้าที่ที่ได้รับมอบหมาย

๒.๔ การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย ผู้ใช้งานควรปฏิบัติ ดังต่อไปนี้

๒.๔.๑ ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของสำนักงาน อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดแก่สำนักงาน

๒.๔.๒ ไม่คัดลอกโปรแกรมต่างๆ ที่สำนักงาน ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๒.๔.๓ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ของสำนักงาน จะต้องกำหนดโดยเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศเท่านั้น

๒.๔.๔ ไม่ทำการปรับแต่งไบออส (BIOS) หรือการตั้งค่าระบบ (Configuration) อื่นใดที่อาจส่งผลกระทบต่อระบบการทำงานของคอมพิวเตอร์ อันเป็นเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้เป็นปกติ

๒.๔.๕ ไม่ทำการเปลี่ยนแปลงเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์แบบตั้งโต๊ะภายในสำนักงาน

๒.๔.๖ หากผู้ใช้งานที่มีความประสงค์จะขอใช้เลขที่อยู่ไอพีสาธารณะ (Public IP Address)จะต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

๒.๔.๗ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่ายเว้นแต่จะได้รับอนุญาตจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

๒.๔.๘ ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของสำนักงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของสำนักงานได้ เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

๒.๔.๙ ไม่ใช้บริการบนระบบอินเทอร์เน็ต (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน

๓. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

๓.๑ เมื่อฝ่ายเทคโนโลยีสารสนเทศ ได้รับการแจ้งผ่านทางจดหมายอิเล็กทรอนิกส์จากฝ่ายบุคคลตามกระบวนการเพื่อจัดหาเครื่องคอมพิวเตอร์ให้กับพนักงานหรือลูกจ้างที่รับใหม่ ฝ่ายเทคโนโลยีสารสนเทศจะทำการสร้าง ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์สำนักงาน ซึ่งเป็นระบบ Active Directory หลังจากนั้นผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่าน (Password) เมื่อทำการลงชื่อเข้า (Login) ครั้งแรก

๓.๒ ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของสำนักงาน

๓.๓ ผู้ใช้งานควรทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานกว่า 30 นาที

๓.๔ มีการกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัยโดยการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and authentication) โดยจะทำการเก็บข้อมูลการทางจราจรคอมพิวเตอร์ (Log) ในกรณีนี้สำนักงาน ได้ใช้ระบบ Active Directory เป็นตัวควบคุม

๔. แนวปฏิบัติการใช้งานบัญชีผู้ใช้งาน (Account)

๔.๑ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้งาน (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้งาน (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๔.๒ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้งาน (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๔.๓ ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้งาน (Account) ของตนเองและทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๕. ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและผ่านการฝึกอบรม หลักสูตร การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต มีรายละเอียด ดังนี้

๕.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม ตัวอย่างเช่น จัดอบรม พรบ.คอมพิวเตอร์โดยผู้เชี่ยวชาญเฉพาะด้าน

๕.๒ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) จัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๕.๓ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) จัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ ตัวอย่างเช่น เมื่อมีเจ้าหน้าที่หรือพนักงานของสำนักงานลาออกจากงานไปแล้วโดยปกติ จะต้องทำการเก็บข้อมูลไว้ระยะหนึ่งตามความเหมาะสมและความเห็นของผู้มีอำนาจตามสายงานนั้นๆ ซึ่งเมื่อถึงระยะรอบเวลาดังกล่าว ฝ่ายเทคโนโลยีสารสนเทศจะทำการสอบถามไปยังผู้มีอำนาจตามสายงาน โดยวิธีต่างๆ อย่างเช่น จดหมายอิเล็กทรอนิกส์ (e-mail) หรือ บันทึกข้อความ ทั้งนี้ขึ้นอยู่กับความเหมาะสม ของแต่ละครั้งไป

๖. แนวปฏิบัติการใช้รหัสผ่าน (Password)

๖.๑ รหัสผ่าน (Password) ควรมีความยาวไม่น้อยกว่า ๖ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่างๆด้วย ควรใช้อักขระพิเศษประกอบ เช่น : ; < > เป็นต้น

๖.๒ ไม่ควรกำหนดรหัสผ่าน (Password) จากชื่อ หรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์ และไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” หรือ “123456” เป็นต้น

๖.๓ ทำการเปลี่ยนรหัสผ่าน (Password) เพื่อใช้งานเครื่องคอมพิวเตอร์ของสำนักงานทุก ๓-๖ เดือน หรือเปลี่ยนรหัสผ่าน (Password) ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

๖.๔ ในการเปลี่ยนรหัสผ่านแต่ละครั้ง ไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย

๖.๕ ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรก (default password) หรือได้รับรหัสผ่านใหม่ควรเปลี่ยนรหัสผ่านนั้นโดยทันที

๖.๖ ผู้ใช้งานเก็บรักษารหัสผ่าน (Password) สำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มา โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๖.๗ หากมีการนำอุปกรณ์สื่อสารสนเทศอื่นๆเข้ามาต่อพวงอย่างเช่น แฟลชไดร์ฟ, สมาร์ทโฟน, กล้องดิจิตอล ผู้ใช้งานจะต้องแน่ใจว่าอุปกรณ์เหล่านั้นไม่ก่อให้เกิดความเสียหายต่ออุปกรณ์คอมพิวเตอร์ภายในสำนักงาน หากจำเป็นต้องมีการเชื่อมต่อควรแจ้งเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศเพื่อทำการตรวจสอบก่อนการใช้งาน

๗. แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต (Internet)

๗.๑ ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่สำนักงานคณะกรรมการกำกับกิจการพลังงาน จัดสรรไว้เท่านั้น และห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรแล้ว

๗.๒ ผู้ใช้งานต้องเข้าถึงระบบเทคโนโลยีสารสนเทศ ตามสิทธิ์ที่ได้รับตามหน้าที่ความรับผิดชอบเท่านั้น และเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของสำนักงาน ต้องไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของสำนักงานเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนาพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับสำนักงาน

๗.๓ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงาน ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๗.๔ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) ซึ่งรวมถึงการดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๗.๕ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสำนักงาน

๗.๖ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เสนอความคิดเห็น ใช้ข้อความที่ยั่วยุ ให้ร้าย อันจะก่อให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงานหรือการทำลายความสัมพันธ์กับบุคลากรของสำนักงาน

๗.๗ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้ใช้งานควรทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

๘. แนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๑ แนวปฏิบัติการใช้งานสำหรับผู้ใช้งาน

๘.๒.๑ เมื่อฝ่ายเทคโนโลยีสารสนเทศได้รับจดหมายอิเล็กทรอนิกส์จากฝ่ายบริหารงานบุคคลเพื่อแจ้งให้ทราบถึงรายละเอียดของ พนักงานหรือลูกจ้างในสำนักงาน เป็นที่เรียบร้อยแล้วนั้น ฝ่ายเทคโนโลยีสารสนเทศจะดำเนินการสร้างชื่อผู้ใช้งานพร้อมรหัสผ่านให้กับพนักงานหรือลูกจ้างในสำนักงาน โดยเป็นความลับเฉพาะเพื่อใช้งานจดหมายอิเล็กทรอนิกส์

๘.๒.๒ ผู้ใช้งานที่ได้รับรหัสผ่าน (Password) ครั้งแรกในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นจะต้องเปลี่ยนรหัสผ่าน (Password) โดยทันที

๘.๒.๓ ผู้ใช้งานไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๘.๒.๔ ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่าน (Password) ทุก ๓-๖ เดือนหรือตามระยะเวลาที่เหมาะสม

๘.๒.๕ ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ เว้นแต่จะได้รับความยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ (e-mail) ของตน

๘.๒.๖ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นผู้ใช้งานควรทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้ามาสวมสิทธิ์การใช้งาน

๘.๒.๗ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

๘.๒.๘ ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๘.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ

๘.๒.๑ ผู้ดูแลระบบได้กำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของสำนักงาน ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การโอนย้าย โดยจะต้องได้รับหนังสือจากต้นสังกัดของผู้ใช้งานเพื่อยืนยันการเพิ่ม ลดสิทธิ์รวมไปถึงการทำลายข้อมูลเป็นต้น

๘.๒.๒ ผู้ดูแลระบบได้กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๑๐ ครั้งหรือขึ้นอยู่กับความเหมาะสมกับระบบนั้นๆ

๙. แนวปฏิบัติให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(Application and Information Access Control) โดยมีรายละเอียด ดังนี้

๙.๑ มีการจำกัดการเข้าถึงสารสนเทศ (Information access restriction) หรือควบคุมการเข้าถึงการใช้งานของผู้ใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่นตามความเหมาะสมหรือตามหน้าที่ ที่ได้รับมอบหมาย

๙.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร จะได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ อย่างเช่น ระบบบริหารทรัพยากรบุคคล เป็นต้น

๙.๓ การควบคุมคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ได้กำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารตามความเหมาะสม

๙.๔ การควบคุมการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) หรือ การควบคุมระยะไกล (Remote Desktop) กำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานภายนอกสำนักงาน ทั้งนี้สำนักงานจะให้บริการในส่วนนี้ผ่านทางหน้าเว็บไซต์ซึ่งจะมีระบบไฟร์วอลล์ (Firewall) เป็นตัวควบคุมและบริหารจัดการการส่ง-รับข้อมูลผ่านการทำงานประเภทการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) หรือการควบคุมระยะไกล (Remote Desktop)

ส่วนที่ ๓

แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายของสำนักงาน และป้องกันการบุกรุกผ่านระบบเครือข่าย หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของสำนักงาน ได้อย่างถูกต้อง

๒. แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ

๒.๑ ฝ่ายเทคโนโลยีสารสนเทศ ได้กำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศของสำนักงาน เพื่อดูแลรักษาความปลอดภัย โดยบุคคล ภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของสำนักงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

๒.๒ ผู้ดูแลระบบ (System Administrator) ได้กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างน้อยปีละ ๑ ครั้ง

๒.๓ ผู้ดูแลระบบ (System Administrator) ได้จัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของสำนักงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

๒.๔ ผู้ดูแลระบบ (System Administrator) ได้จัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๓. แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบสารสนเทศ

ฝ่ายเทคโนโลยีสารสนเทศ ผู้ดูแลระบบ (System Administrator) ได้กำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญเช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งได้มีการทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๓.๑ ผู้ดูแลระบบได้บริหารจัดการสิทธิ์ของผู้ใช้งาน ดังต่อไปนี้

๓.๑.๑ กำหนดจำแนกประเภทสิทธิ์ตามหน้าที่และความรับผิดชอบ โดยจัดเก็บและมอบหมายสิทธิ์ให้แก่ผู้ใช้งานระบบสารสนเทศซึ่งจะมีสิทธิ์ตามลำดับชั้นการเข้าถึงข้อมูล ดังนี้

๓.๑.๑.๑ กรรมการ (คณะกรรมการกำกับกิจการพลังงาน)

๓.๑.๑.๒ ผู้บริหารระดับสูง (เลขาธิการ,รองเลขาธิการ,ผู้ช่วยเลขาธิการ)

๓.๑.๑.๓ ผู้บริหารระดับอาวุโส (ผู้อำนวยการฝ่าย)

๓.๑.๑.๔ ผู้บริหารระดับกลาง (ผู้อำนวยการส่วน)

๓.๑.๑.๕ ระดับผู้ชำนาญการ (ผู้ชำนาญการพิเศษ)

๓.๑.๑.๖ ระดับวิชาการ (เจ้าหน้าที่วิชาการ)

๓.๑.๑.๗ ระดับปฏิบัติการ (เจ้าหน้าที่ทั่วไป)

๓.๑.๑.๘ ลูกจ้าง (ลูกจ้างเหมาบริการ,พนักงานช่วยอำนวยการ)

๓.๑.๑.๙ ที่ปรึกษา (ที่ปรึกษาโครงการ)

๓.๑.๑.๑๐ ผู้ดูแลระบบ ในที่นี้หมายถึง เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศสำนักงาน

๓.๑.๒ ในกรณีผู้ใช้งานมีความจำเป็นต้องใช้สิทธิ์สูงกว่าปกติ ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงข้อมูลระดับใดได้บ้าง โดยกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติเพื่อผู้ดูแลระบบจะได้ดำเนินการปรับค่าหรือแก้ไขต่อไป

๓.๑.๓ ทำการยกเลิกรหัสผ่าน (Password) เมื่อได้รับการแจ้งจากส่วนบริหารงานบุคคลหรือผู้อำนวยการฝ่าย เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่งหรือยกเลิกอำนาจหน้าที่

๔. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๔.๑ ผู้ดูแลระบบ (System Administrator) ดำเนินการควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access- Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๔.๒ ผู้ดูแลระบบ (System Administrator) ดำเนินการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๔.๓ ผู้ดูแลระบบ (System Administrator) ดำเนินการกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สายตามความเหมาะสมในกรณีต่างๆ

๔.๔ ผู้ดูแลระบบ (System Administrator) ใช้วิธีการควบคุมผ่านระบบ AD (Active Directory) โดยกำหนดชื่อผู้ใช้ (Username) รหัสผ่าน (Password) สำหรับพนักงานและลูกจ้างในสำนักงาน และใช้วิธีการควบคุมผ่านระบบ Firewall Authentication โดยกำหนดชื่อผู้ใช้ (Username) รหัสผ่าน (Password) สำหรับบุคคลภายนอก

๔.๕ ผู้ดูแลระบบ (System Administrator) ติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในสำนักงาน

๔.๖ ผู้ดูแลระบบ (System Administrator) ได้กำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

๔.๗ ผู้ดูแลระบบ (System Administrator) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบทันที

๔.๘ ผู้ดูแลระบบ (System Administrator) ควบคุมดูแลไม่ให้บุคคลภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของสำนักงาน

๕. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

๕.๑ ฝ่ายเทคโนโลยีสารสนเทศได้กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ไม่ใช่เจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ โดยต้องลงทะเบียนขออนุญาต ระบุ วัน-เวลา เข้าออกและเหตุผลความจำเป็น

๕.๒ ผู้ใช้งานภายนอกที่จะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของสำนักงาน ต้องได้รับอนุญาตจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๕.๓ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

๕.๔ ผู้ดูแลระบบ (System Administrator) ควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

๕.๔.๑ ใช้วิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๔.๒ มีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๕.๔.๓ มีการกำหนดให้จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ของผู้ใช้งานไปยังเครื่องคอมพิวเตอร์แม่ข่าย

๕.๔.๔ ระบบเครือข่ายทั้งหมดของสำนักงาน ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกสำนักงาน ได้ถูกเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก และมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware)

๕.๔.๕ การเข้าสู่ระบบเครือข่ายภายในสำนักงาน ผ่านทางระบบอินเทอร์เน็ตได้กำหนดให้ลงบันทึกเข้า (Login) โดยระบุชื่อผู้ใช้งานและรหัสผ่านผู้ใช้งานผ่านระบบพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้งาน

๕.๔.๖ เลขที่อยู่ไอพี (IP Address) ของระบบเครือข่ายภายในสำนักงาน ได้มีการป้องกันหน่วยงานภายนอกที่เชื่อมต่อ ไม่สามารถมองเห็นได้

๕.๔.๗ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก ที่สามารถระบุบนระบบเครือข่ายและอุปกรณ์บนเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอและการระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) มีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๕.๔.๘ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย จะต้องได้รับการอนุมัติจากผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๔.๙ มีการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ควบคุมการเข้าถึง

พอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๕.๔.๑๐ มีการควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

๕.๔.๑๑ มีการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๕.๕ ผู้ดูแลระบบ (System Administrator) ทำหน้าที่บริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

๕.๖ ฝ่ายเทคโนโลยีสารสนเทศได้กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

๕.๖.๑ ความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ กำหนดชั้นความลับในการเข้าถึงข้อมูลซึ่งผู้ดูแลระบบไม่ได้รับอนุญาตให้แก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของสำนักงาน (Internal IT Auditor) หรือบุคคลที่สำนักงานมอบหมาย

๕.๖.๒ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

๕.๖.๓ ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๕.๖.๔ วิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๕.๗ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

๕.๗.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของสำนักงาน จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

๕.๗.๒ ผู้ดูแลระบบได้ควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๕.๗.๓ วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

๕.๗.๔ การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ

๕.๗.๕ การเข้าใช้งานต้องผ่านระบบการพิสูจน์ตัวตนจากระบบของสำนักงาน

๖. แนวปฏิบัติการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

ฝ่ายเทคโนโลยีสารสนเทศได้กำหนดมาตรการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของสำนักงาน ในขณะที่ไม่มีผู้ดูแล ดังต่อไปนี้

๖.๑ ผู้ใช้งานต้องออกจาก (Log out) ระบบสารสนเทศโดยทันทีเมื่อเสร็จสิ้นการใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานๆ

๖.๒ ป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบสารสนเทศของตน

๖.๓ สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกันการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

๖.๔ เมื่อผู้ใช้งานระบบสารสนเทศทิ้งไว้โดยไม่ใช้งานเป็นเวลานาน ระบบจะยุติการใช้งานระบบภายในระยะเวลา 10 นาที หรือตามความเหมาะสมขึ้นอยู่กับระบบนั้นๆ

๗. แนวปฏิบัติการลงทะเบียนผู้ใช้งาน

ผู้ดูแลระบบ (System Administrator) จัดทำขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานในการเข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว ดังต่อไปนี้

๗.๑ ทำการลงทะเบียนผู้ใช้งาน สำหรับระบบสารสนเทศของสำนักงาน ตามเอกสารหรือ จดหมายอิเล็กทรอนิกส์ (e-mail) ที่ได้รับแจ้งเป็นลายลักษณ์อักษรจากต้นสังกัดนั้นๆ

๗.๒ ตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๗.๓ ตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามข้อกำหนดของต้นสังกัด

๗.๔ แสดงเอกสารเป็นบันทึกหรือจดหมายอิเล็กทรอนิกส์ (e-mail) แจ้งให้แก่ผู้ใช้งานเพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศ

๗.๕ กำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๗.๖ การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมดเพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่รับอนุญาต

๘. แนวปฏิบัติการดูแลสินทรัพย์สารสนเทศ

๘.๑ ผู้ดูแลระบบ (System Administrator) ทำหน้าที่ควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือเทปบันทึก Back up ข้อมูล ซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิจัดเก็บไว้ในที่ที่ปลอดภัยในเวลาที่ไม่มีผู้ดูแล และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๘.๒ ผู้ใช้งานต้องจัดเก็บข้อมูลสารสนเทศที่มีความสำคัญหรือเป็นความลับของสำนักงาน ไว้ในที่ปลอดภัยภายหลังจากใช้งานเสร็จ

๘.๓ ผู้ใช้งานต้องป้องกันไม่ให้บุคคลภายนอกใช้กล้องดิจิตอล เครื่องสำเนาเอกสาร และเครื่องสแกนเอกสาร โดยไม่ได้รับอนุญาต

๙. แนวปฏิบัติการแบ่งแยกระบบเครือข่าย

ผู้ดูแลระบบ (System Administrator) ดำเนินการแบ่งแยกระบบเครือข่าย เป็นกลุ่มของผู้ใช้บริการและกลุ่มของระบบสารสนเทศ เพื่อจำกัดสิทธิการใช้งาน และควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น โดยแบ่งออกเป็น ๓ โซน ดังต่อไปนี้

๙.๑ โซนเครื่องคอมพิวเตอร์แม่ข่าย เป็นโซนที่มีการจัดเตรียมอุปกรณ์ และระบบเพื่อป้องกันและรักษาความมั่นคงปลอดภัยในระดับสูง เช่น ระบบตรวจจับและป้องกันผู้บุกรุก ระบบสำรองไฟฟ้า ระบบสำรองข้อมูล

๙.๒ โซนผู้ใช้งานภายในเป็นโซนสำหรับบุคคลากรในสำนักงานโดยมีการติดตั้งระบบ Antivirus และระบบ Firewall

๙.๓ โซนภายนอก สำหรับบุคคลภายนอกให้สามารถเข้าถึงและใช้งานสารสนเทศภายในหน่วยงานผ่านอุปกรณ์ระบบรักษาความปลอดภัย Firewall หรือ (Intrusion Prevention System/Intrusion Detection System)

ส่วนที่ ๔

แนวปฏิบัติของผู้ดูแลระบบ

๑. วัตถุประสงค์

เพื่อกำหนดหน้าที่และแนวปฏิบัติของผู้ดูแลระบบ (System Administrator) ในการบริหารจัดการ กำกับ ดูแลเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย (Network) ให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งการสอดส่องดูแลผู้ใช้งานให้เป็นไปตามแนวนโยบาย

๒. แนวปฏิบัติของผู้ดูแลระบบ (System Administrator)

๒.๑ ผู้ดูแลระบบ (System Administrator) มีอำนาจหน้าที่ ดังต่อไปนี้

๒.๑.๑ ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของสำนักงาน ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่สำนักงาน ให้ผู้ดูแลระบบ (System Administrator) พิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้งานดังกล่าวได้ทันที

๒.๑.๒ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่ายอยู่เสมอ

๒.๑.๓ ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๒.๑.๔ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย

๒.๑.๕ เมื่อหมดความจำเป็นในการใช้งาน ด้วยวิธีการตามมาตรฐาน DOD 5220.22-M ผู้ดูแลระบบจะทำการลบข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์แม่ข่าย (Server) อย่างถาวร หรือทำลายข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของสำนักงาน บนเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒.๑.๖ ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๒.๑.๗ ดูแลรักษาและปรับปรุงบัญชีจดหมายอิเล็กทรอนิกส์ (e-mail) ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิ์การใช้งานของผู้ใช้งานที่พ้นสภาพการเป็นผู้ใช้งาน

๒.๑.๘ ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้งานให้มีการกำหนดรหัสผ่าน (Password) รวมทั้งการเก็บรักษารหัสผ่าน (Password)

๒.๑.๙ ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

๒.๑.๑๐ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

๒.๑.๑๑ ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๒.๑.๑๒ เมื่อผู้ดูแลระบบ (System Administrator) พ้นจากหน้าที่ จะต้องคืนสินทรัพย์ของสำนักงาน ที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายตรวจสอบการคืนสินทรัพย์

๒.๒ ผู้ดูแลระบบ (System Administrator) ทำหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้บริการและเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

๒.๒.๑ เก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้

๒.๒.๒ มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบ (System Administrator) สามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของสำนักงาน (Internal IT Auditor) หรือบุคคลที่สำนักงานมอบหมาย

๒.๒.๓ ในการเก็บข้อมูลจราจรนั้น สามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

๒.๒.๔ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริง ผู้ดูแลระบบได้ตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ส่วนที่ ๕

แนวปฏิบัติการจัดทำระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉิน

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมในกรณีเกิดเหตุฉุกเฉินหรือไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ตามปกติอย่างต่อเนื่อง เหมาะสม และสอดคล้องกับการใช้งานตามภารกิจของสำนักงาน

๒. แนวปฏิบัติการสำรองข้อมูล

๒.๑ ฝ่ายเทคโนโลยีสารสนเทศสำรองข้อมูลและซอฟต์แวร์เก็บไว้บนเทปบันทึกข้อมูล เป็นรายวัน รายสัปดาห์ รายเดือน รายปี โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของสำนักงาน จากจำเป็นมากไปหาน้อย

๒.๒ ฝ่ายเทคโนโลยีสารสนเทศจัดทำขั้นตอนการปฏิบัติการและจัดทำการสำรองข้อมูลและการกู้คืนข้อมูลอย่างสม่ำเสมอทุกเดือนหรือตามความเหมาะสมไปยังศูนย์กู้คืนระบบจากความเสียหายทางภัยพิบัติ (DR-Site) ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

๒.๓ ฝ่ายเทคโนโลยีสารสนเทศได้จัดเก็บเทปที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจนและทำการจัดเก็บเทปสำรองข้อมูลรายเดือนแยกไว้ ณ สถานที่อื่น

๒.๔ ฝ่ายเทคโนโลยีสารสนเทศได้เตรียมศูนย์คอมพิวเตอร์สำรอง (DR site) เพื่อเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบงานตามลำดับความสำคัญคืนมาให้ใช้งานได้ภายในระยะเวลาที่เหมาะสม โดยมีการทดสอบปีละ ๒ ครั้ง

๒.๕ มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เป็นลำดับชั้น โดยผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศเป็นผู้กำกับดูแลการปฏิบัติงาน

ส่วนที่ ๖

แนวปฏิบัติการประเมินความเสี่ยง

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

๒. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง

๒.๑ ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของสำนักงาน เพื่อการตรวจสอบและประเมินความเสี่ยงนั้น ดังต่อไปนี้

- ๒.๑.๑ ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)
- ๒.๑.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต
- ๒.๑.๓ ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน
- ๒.๑.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกันมากกว่าหนึ่งจุด
- ๒.๑.๕ ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต
- ๒.๑.๖ จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒.๒ กำหนดวิธีการในการตรวจสอบและประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๒.๓ การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

- ๒.๓.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ
- ๒.๓.๒ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น
- ๒.๓.๓ จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ
- ๒.๓.๔ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในสำนักงาน เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ ความเสียหายหรืออันตรายที่จะเกิดขึ้นของหน่วยงาน

ส่วนที่ ๗

แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของสำนักงาน

๒.๒ จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้

๒.๓ ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ส่วนที่ ๘

การกำหนดผู้รับผิดชอบ

กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. ระดับนโยบาย

ให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานที่ทำหน้าที่ CIO และผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานคณะกรรมการกำกับกิจการพลังงาน ติดตามและกำกับดูแล ควบคุมตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติ

๒. แนวทางปฏิบัติของผู้รับผิดชอบ

๒.๑ ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงานอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการ รวมทั้งรับผิดชอบ ดังนี้

- ๒.๑.๑ ควบคุมการเข้า-ออกห้อง Server ตามการกำหนดสิทธิการเข้าถึง Server
- ๒.๑.๒ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม.
- ๒.๑.๓ กำกับดูแล การติดตั้ง รื้อถอน ดูแล ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN , Internet , Intranet ที่ให้บริการในสำนักงาน
- ๒.๑.๔ กำกับดูแลรักษาการทำงานระบบดับเพลิงอัตโนมัติของเครื่อง Server ให้สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้
- ๒.๑.๕ แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ
- ๒.๑.๖ รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาระดับสูงทราบสม่ำเสมอ
- ๒.๑.๗ กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ
- ๒.๑.๘ กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

ตามแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานคณะกรรมการกำกับกิจการพลังงาน

๒.๑.๙ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ใน Server ของระบบฐานข้อมูลทั้งหมดที่ให้บริการในเว็บไซต์ ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม.

๒.๑.๑๐ กำกับดูแล ตรวจสอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบอื่น ๆ