

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักงานป้องกันและปราบปรามการฟอกเงิน

พ.ศ. ๒๕๖๕

ศูนย์เทคโนโลยีสารสนเทศ

สำนักงานป้องกันและปราบปรามการฟอกเงิน

คำนำ

สำนักงานป้องกันและปราบปรามการฟอกเงิน ได้ออกประกาศเรื่องนโยบายในการรักษาความปลอดภัย พ.ศ. ๒๕๕๔ และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๔ เพื่อให้มีแนวทางการรักษาความมั่นคงปลอดภัยสารสนเทศในการให้บริการอิเล็กทรอนิกส์ภาครัฐและเพื่อให้สอดคล้องตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

ในปีงบประมาณ พ.ศ. ๒๕๖๕ ศูนย์เทคโนโลยีสารสนเทศได้ทำการทบทวนและปรับปรุงเนื้อหาเพิ่มเติมให้เป็นปัจจุบัน และแนวปฏิบัติที่กำหนดต่อไปนี้ เป็นสิ่งสำคัญที่ผู้ปฏิบัติงานต้องถือปฏิบัติเพื่อให้การให้บริการต่างๆ ตามภารกิจของสำนักงานป้องกันและปราบปรามการฟอกเงิน ที่ดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ และเพื่อให้ง่ายต่อการนำไปปฏิบัติหรืออ้างอิง จึงแบ่งแนวปฏิบัติออกเป็น ๑๑ หมวด ดังนี้

หมวด ๑ แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ
หมวด ๒ แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึงของผู้รับผิดชอบระบบ
หมวด ๓ แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ
หมวด ๔ แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน
หมวด ๕ แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบ/ผู้ดูแลเครือข่าย
หมวด ๖ แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย
หมวด ๗ แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการของผู้ใช้งาน
หมวด ๘ แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน
หมวด ๙ แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย
หมวด ๑๐ แนวปฏิบัติในการจัดซื้อจัดจ้างระบบสารสนเทศ
หมวด ๑๑ แนวปฏิบัติในการเผยแพร่ข้อมูลต่อสาธารณะ

สารบัญ

คำนำ..... ก

สารบัญ..... ข

หมวด ๑ แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ..... ๑

หมวด ๒ แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึงของผู้รับผิดชอบระบบ..... ๕

หมวด ๓ แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ..... ๗

หมวด ๔ แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน..... ๑๑

หมวด ๕ แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบ/ผู้ดูแลเครือข่าย..... ๑๕

หมวด ๖ แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย..... ๑๖

หมวด ๗ แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการของผู้ใช้งาน..... ๒๐

หมวด ๘ แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน..... ๒๑

หมวด ๙ แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย..... ๒๒

หมวด ๑๐ แนวปฏิบัติในการจัดซื้อจัดจ้างระบบสารสนเทศ ๒๔

หมวด ๑๑ แนวปฏิบัติในการเผยแพร่ข้อมูลต่อสาธารณะ..... ๒๗

ภาคผนวก ก คู่มือการลงทะเบียนผู้ใช้งาน (User Registration) สำนักงาน ปปง. ก-๑

หมวด ๑

แนวปฏิบัติในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของสำนักงานป้องกันและปราบปรามการฟอกเงิน (สำนักงาน ปปง.) ต้องมีหน้าที่บริหารจัดการควบคุมการเข้าถึงระบบสารสนเทศ ดังนี้

๑.๑ ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศได้ ก็ต่อเมื่อได้รับอนุญาตจากผู้ดูแลระบบ หรือผู้รับผิดชอบระบบงานตามหน้าที่การปฏิบัติงานเท่านั้น

๑.๒ ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบ กล่าวคือ ในการขออนุญาตเข้าใช้งานระบบงาน ผู้ใช้จะต้องทำบันทึกและกรอกเอกสารที่สำนักงาน ปปง. กำหนด เพื่อขอเข้าใช้งานระบบและให้ผู้บังคับบัญชา หรือผู้รับมอบอำนาจจากผู้บังคับบัญชาลงนามอนุมัติเอกสารดังกล่าว เพื่อจัดเก็บไว้เป็นหลักฐาน จากนั้นผู้ดูแลระบบจะสร้างบัญชีสำหรับการเข้าถึงโดยอนุญาตเฉพาะในส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับเป็นหลัก

๑.๓ ผู้ดูแลระบบต้องกำหนดไม่ให้ผู้ใช้งานเข้าสู่ระบบได้ หากผู้ใช้งานใส่รหัสผ่านเพื่อเข้าใช้งานผิด ๓ ครั้ง ระบบจะยกเลิกสิทธิการใช้งาน (Block) ไม่ให้ผู้ใช้งานสามารถใช้งานได้จนกว่าผู้ใช้งานจะยื่นเรื่องพร้อมหลักฐานแสดงต่อเจ้าหน้าที่ดูแลระบบ เพื่อขอรหัสใหม่อีกครั้ง

๑.๔ ผู้ดูแลระบบต้องกำหนดให้มีการเข้าใช้ระบบ (Login) เพื่อเข้าใช้งานใด ๆ จะต้องมีการตรวจจับการเปิดระบบงานไว้ เมื่อไม่มีการใช้งานก็ต้องออกจากระบบ (Logout) หรือให้ออกจากระบบ (Logout) อัตโนมัติตามระยะเวลาที่เหมาะสม

๑.๕ ผู้ดูแลระบบต้องอนุญาตให้ผู้ใช้งานเข้าถึงโปรแกรมประยุกต์ หรือแอปพลิเคชันและระบบสารสนเทศ ในส่วนที่จำเป็นตามหน้าที่การปฏิบัติงานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำ เท่านั้น

๑.๖ กรณีมีการจ้างผู้ให้บริการภายนอก (Outsource) ในการพัฒนา ดูแล และบำรุงรักษาระบบสารสนเทศ หรือแอปพลิเคชัน มีมาตรการควบคุม ดังนี้

(๑) กำหนดเกณฑ์และคัดเลือกผู้ให้บริการภายนอกที่มีคุณสมบัติตรงตามมาตรฐานที่หน่วยงานต้องการและมีขั้นตอนการปฏิบัติงานที่รอบคอบ รัดกุมและน่าเชื่อถือ

(๒) กำหนดข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้ให้บริการภายนอกและต้องระบุการรักษาความลับของข้อมูล กำหนดขอบเขตงานและเงื่อนไขในการให้บริการอย่างชัดเจน

(๓) กรณีใช้บริการด้านการพัฒนาระบบงาน กำหนดให้ผู้ให้บริการภายนอกเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงานเท่านั้นและหากมีความจำเป็นที่ผู้ให้บริการภายนอกเข้ามาปฏิบัติหน้าที่ภายในสำนักงาน ปปง. ต้องมีเจ้าหน้าที่ของหน่วยงานควบคุมดูแลอย่างใกล้ชิด

(๔) กำหนดให้ผู้ให้บริการภายนอกจัดทำคู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

(๕) กำหนดให้ผู้ให้บริการภายนอกรายงานแผนและผลการปฏิบัติงาน ปัญหาและอุปสรรคต่างๆ และแนวทางในการแก้ไขปัญหาที่เกิดขึ้น

(๖) กำหนดให้มีหลักเกณฑ์ กระบวนการและขั้นตอนในการตรวจรับงานที่ส่งมอบโดยผู้ให้บริการภายนอกที่ชัดเจน

ข้อ ๒ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องมีหน้าที่บริหารจัดการรักษาความปลอดภัยทางกายภาพ (Physical Security Management) ดังนี้

๒.๑ กำหนดระดับความสำคัญของพื้นที่ หรือจำแนกพื้นที่การใช้งานกับพื้นที่การควบคุม

๒.๒ ทดสอบระบบควบคุมการเข้าถึงพื้นที่ทางกายภาพ เพื่อให้ทราบว่าระบบยังใช้งานได้ตามปกติหรือไม่

๒.๓ ผู้ปฏิบัติงานควรปิดประตูและหน้าต่างให้สนิทอยู่เสมอ

ข้อ ๓ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องมีหน้าที่บริหารจัดการควบคุมพื้นที่การเข้า – ออก พื้นที่การควบคุม ได้แก่ ห้องปฏิบัติการคอมพิวเตอร์ ดังนี้

๓.๑ มีการบันทึกวันและเวลาการเข้า – ออก พื้นที่การควบคุมของผู้มาเยือน (Visitor)

๓.๒ ดูแลผู้มาเยือนในพื้นที่ หรือบริเวณที่มีการควบคุมจนกระทั่งเสร็จสิ้นภารกิจและกลับไปเพื่อป้องกันการสูญหายของทรัพย์สิน หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๓.๓ จัดให้มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของสำนักงาน ปปง. โดยบุคคลภายนอกและควรมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๓.๔ จัดสื่อประชาสัมพันธ์เพื่อสร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์ หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๓.๕ มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บ หรือประมวลผลอยู่

๓.๖ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่ หรือบริเวณที่มีความสำคัญ เว้นแต่ได้รับอนุญาต

๓.๗ มีการพิสูจน์ตัวตน ได้แก่ การแสดงบัตรผ่าน การใช้บัตรแถบแม่เหล็ก การสแกนลายนิ้วมือ การสแกนเส้นเลือดดำบนฝ่ามือ (Palm Vein Pattern) เป็นต้น โดยเฉพาะห้องปฏิบัติการคอมพิวเตอร์ เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ

๓.๘ จัดเก็บบันทึกการเข้า-ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ โดยเฉพาะห้องปฏิบัติการคอมพิวเตอร์ เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๓.๙ บุคคลภายนอก ได้แก่ เจ้าหน้าที่บริษัท นักศึกษาฝึกงานหรือผู้ได้รับการว่าจ้างอื่น ๆ ต้องติดบัตรให้เห็นเด่นชัด ตลอดระยะเวลาการทำงาน

๓.๑๐ ผู้มาเยือนต้องติดบัตรให้เห็นเด่นชัด ตลอดระยะเวลาที่อยู่ภายในสำนักงาน ปปง.

๓.๑๑ ควรจัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่ หรือบริเวณที่มีความสำคัญ

๓.๑๒ จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

ข้อ ๔ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องกำหนดการจัดวางและการป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง (Hardware) ดังนี้

๔.๑ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงของบุคคลภายนอก

๔.๒ ระบบงานที่มีความสำคัญให้แยกเก็บไว้อีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัยเพียงพอ

๔.๓ ไม่ให้มีการนำอาหาร เครื่องดื่ม หรือสูบบุหรี่ภายในบริเวณห้องปฏิบัติการคอมพิวเตอร์

๔.๔ ตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณ หรือพื้นที่ที่มีระบบสารสนเทศ อยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว ได้แก่ การตรวจสอบระดับอุณหภูมิ ความชื้น ให้อยู่ในระดับปกติอยู่เสมอ

ข้อ ๕ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องกำหนดให้มีระบบป้องกันและสนับสนุนการทำงาน ดังนี้

๕.๑ มีระบบสนับสนุนการทำงานของระบบสารสนเทศที่เพียงพอต่อความต้องการใช้งาน โดยให้มีอย่างน้อย ดังนี้

(๑) ระบบสำรองกระแสไฟฟ้า (UPS)

(๒) ระบบระบายอากาศ

(๓) ระบบปรับอากาศและควบคุมความชื้น

(๔) ระบบดับเพลิงอัตโนมัติ

(๕) ระบบกล้องวงจรปิด

๕.๒ ให้มีการตรวจสอบ หรือทดสอบระบบสนับสนุนอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๕.๓ ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องปฏิบัติการคอมพิวเตอร์ทำงานผิดปกติ หรือหยุดการทำงาน

ข้อ ๖ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องกำหนดและควบคุมการเดินสายไฟ สายสัญญาณการสื่อสาร และสายเคเบิ้ลอื่นๆ ดังนี้

๖.๑ เครือข่ายภายในสำนักงาน ปปง. ในลักษณะที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ ต้องให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณและป้องกันสัตว์ต่างๆ กัดสาย ได้แก่ หนู แมลงสาบ เป็นต้น ซึ่งจะทำให้เกิดความเสียหายต่อสายสัญญาณ

๖.๒ ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณ ซึ่งกันและกัน

๖.๓ จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

๖.๔ ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

ข้อ ๗ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องกำหนดการบำรุงรักษาอุปกรณ์ดังนี้

๗.๑ กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

๗.๒ ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๗.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๗.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๗.๕ ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับจ้างเหมาบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในสำนักงาน ปปง.

๗.๖ จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่เข้าทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๘ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องควบคุมการนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่น ๆ (Hardware) ออกจากสำนักงาน ปปง. ดังนี้

๘.๑ ให้มีการขออนุญาตก่อนนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่น ๆ (Hardware) ออกจากสำนักงาน ปปง.

๘.๒ บันทึกข้อมูลการนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆ (Hardware) ออกจากสำนักงาน ปปง. เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำส่งคืน

ข้อ ๙ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องบริหารจัดการควบคุมอุปกรณ์ที่ใช้งานอยู่ภายนอกสำนักงาน ปปง. ดังนี้

๙.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆ (Hardware) ของสำนักงาน ปปง. ออกไปใช้งานนอกสถานที่ ดังนี้

(๑) ห้ามผู้ใช้งานละทิ้งเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆ (Hardware) ของสำนักงาน ปปง. ไว้โดยลำพัง ในที่สาธารณะ

(๒) ให้ผู้ใช้งานรับผิดชอบดูแลเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงอื่นๆ (Hardware) ของสำนักงาน ปปง. เสมือนเป็นทรัพย์สินของตนเอง

ข้อ ๑๐ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องควบคุมการจำหน่ายอุปกรณ์จัดเก็บข้อมูล หรือการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง ดังนี้

๑๐.๑ ให้ทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะแทงจำหน่ายอุปกรณ์ดังกล่าว ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูล ในหมวด ๓ แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ ข้อ ๑ (๑๒)

๑๐.๒ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์จัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

ข้อ ๑๑ ผู้ใช้งานต้องเข้าร่วมการฝึกอบรมความตระหนักและความรู้เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศแก่ผู้ใช้งานเป็นประจำ อย่างน้อยปีละ ๑ ครั้ง ดังนี้

๑๑.๑ หลักสูตรสร้างความเข้าใจอันดีแก่ผู้ใช้งานถึงแนวนโยบายและแนวปฏิบัติเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

๑๑.๒ หลักสูตรความตระหนักและทักษะเพื่อความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงมาตรการเชิงป้องกันตามความเหมาะสม

หมวด ๒

แนวปฏิบัติในการบริหารจัดการสิทธิการเข้าถึงของผู้รับผิดชอบระบบ

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องบริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน ดังนี้

๑.๑ การลงทะเบียนบุคลากรหรือผู้ปฏิบัติงานใหม่ ต้องปฏิบัติตามคู่มือการลงทะเบียนผู้ใช้งาน (User Registration) ที่สำนักงาน ปปง. กำหนดขึ้น เพื่อให้มีสิทธิในการใช้งานระบบสารสนเทศตามความจำเป็นรวมทั้งปฏิบัติตามขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน ได้แก่ เมื่อลาออก หรือเมื่อเปลี่ยนตำแหน่งงานภายในสำนักงาน ปปง. เป็นต้น

๑.๒ กำหนดสิทธิการใช้ระบบสารสนเทศ ที่สำคัญ ได้แก่ ระบบสารสนเทศหลักของหน่วยงาน ระบบสารสนเทศที่ให้บริการภายนอก ระบบอินเทอร์เน็ต (Internet) เครือข่ายไร้สาย (Wireless LAN) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๑.๓ กรณีมีความจำเป็นต้องให้สิทธิพิเศษแก่ผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ ประกอบการพิจารณา เพื่อขอความเห็นชอบและการอนุมัติจากผู้บังคับบัญชา

(๑) ควบคุมการใช้งานอย่างเคร่งครัด โดยเฉพาะระบบสารสนเทศ หรือโปรแกรมประยุกต์ (Application) ที่มีความเสี่ยงและมีความสำคัญสูง

(๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓) มีการเปลี่ยนรหัสผ่าน (Password) อย่างเคร่งครัดทุกครั้ง หลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน

๑.๔ การขอสิทธิเข้าใช้ระบบ (Login) สารสนเทศ หน่วยงานต้นสังกัดของผู้ที่จะขอเพิ่มสิทธิใช้งานระบบแจ้งความประสงค์ต่อศูนย์เทคโนโลยีสารสนเทศ และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ (ผอ.ศท.) พิจารณา เพื่ออนุมัติเพิ่มสิทธิการใช้งาน

ข้อ ๒ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) ของผู้ใช้งาน ดังนี้

๒.๑ กำหนดบัญชีชื่อผู้ใช้งานแยกกันเป็นรายบุคคล กล่าวคือ ไม่กำหนดบัญชีชื่อผู้ใช้งานที่ซ้ำซ้อนกัน

๒.๒ ไม่อนุญาตให้ผู้ร้องขอ เข้าใช้ระบบ (Login) จนกว่าจะได้รับอนุมัติแล้วเท่านั้น

๒.๓ จัดเก็บข้อมูลการลงทะเบียน ขอเข้าใช้งานระบบ เพื่อใช้อ้างอิงหรือตรวจสอบข้อมูลในภายหลัง

๒.๔ ทบทวนบัญชีผู้ใช้งานทั้งหมดอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

ข้อ ๓ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องกำหนดให้มีการพิสูจน์ตัวตนผู้ใช้งาน โดยผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานต้องผ่านการพิสูจน์ตัวตนจากระบบ โดยมีแนวทางปฏิบัติ ดังนี้

๓.๑ การแสดงตัวตนด้วยชื่อบัญชีผู้ใช้งาน (User Account)

๓.๒ การพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน (Password)

๓.๓ การเข้าใช้ระบบงานสำคัญของสำนักงาน ปปง. ผ่านเครือข่ายอินเทอร์เน็ต จะมีการตรวจสอบผู้ใช้งานด้วย

๓.๔ การเข้าใช้ระบบงานสำคัญของสำนักงาน ปปง. จากระยะไกล (Remote Access) จะมีการตรวจสอบ เพื่อเพิ่มความปลอดภัยและเพื่อพิสูจน์ตัวตนของผู้ใช้งาน ได้แก่ รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

๓.๕ ในการใช้งานระบบสารสนเทศ เมื่อมีการว่างเว้นจากการใช้งานเกินเวลา ๕ นาที ระบบจะทำการยกเลิกการใช้งานและการเชื่อมต่อเข้าระบบโดยอัตโนมัติ และผู้ใช้ต้องล็อกหน้าจอโดยทันที ขณะไม่มีผู้ดูแลเพื่อป้องกันผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์

ข้อ ๔ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องกำหนดวิธีการใช้รหัสผ่านให้มีความมั่นคงปลอดภัย ดังนี้

๔.๑ การบริหารจัดการรหัสผ่าน มีมาตรการและการควบคุม ดังนี้

(๑) กำหนดให้ต้องเปลี่ยนรหัสผ่านทุก ๖ เดือน

(๒) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวเลข (Numerical Character) ตัวอักษร (Alphabet) และตัวอักขระพิเศษ (Special Character) โดยไม่เป็นวันเดือนปี ข้อความใดที่ง่ายต่อการล่วงรู้ หรือง่ายต่อการคาดเดา

(๓) กรณีผู้ใช้งานเปลี่ยนหน้าที่ความรับผิดชอบหรือลาออกจะต้องเปลี่ยนหรือถอดถอนสิทธินั้นทันทีเมื่อได้รับแจ้ง

(๔) กำหนดให้การเข้าใช้งานระบบครั้งแรก มีการโต้ตอบด้วยการยืนยันตัวตนและเปลี่ยนรหัสผ่านเพื่อเพิ่มความปลอดภัย

๔.๒ การใช้รหัสผ่าน มีมาตรการให้ผู้ใช้งานต้องใช้ด้วยความระมัดระวัง ดังนี้

(๑) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๒) ไม่ใช้โปรแกรมสำนักงานคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

(๓) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๔) กำหนดรหัสผ่านให้ยากต่อการคาดเดา

(๕) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น เนื่องจากความจำเป็นในการปฏิบัติงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๖) กรณีผู้ใช้งานลาออกหรือเปลี่ยนหน้าที่ความรับผิดชอบ ต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศ ทราบทันที

ข้อ ๕ การใช้รหัสผ่านให้ปลอดภัยและรัดกุม มีมาตรการในการปฏิบัติ ดังนี้

๕.๑ แสดงกระบวนการมอบอำนาจหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

๕.๒ มีการกำหนดสิทธิการเข้าถึงตามความจำเป็น

๕.๓ มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๕.๔ มีวิธีเลือกการใช้รหัสผ่านและการใช้งานรหัสผ่านที่มีคุณภาพ

หมวด ๓

แนวปฏิบัติในการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

ข้อ ๑ ผู้บังคับบัญชาหน่วยงานภายในสำนักงาน ปปง. ต้องจัดให้มีวิธีการกำหนดประเภทข้อมูลและจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ ซึ่งเบื้องต้นใช้แนวทางตาม พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และระเบียบที่เกี่ยวข้องในการกำหนดชั้นความลับของข้อมูล จึงกำหนดให้มีแนวทางปฏิบัติ ดังนี้

๑.๑ ผู้ใช้งานต้องแบ่งประเภทของข้อมูลและชั้นความลับของข้อมูลตามที่ศูนย์เทคโนโลยีสารสนเทศ ได้กำหนดชั้นความลับของข้อมูลเป็น ๔ ระดับ ดังนี้

- ชั้นความลับ (Top secret/Secret/Confidential)
- ใช้ภายในเท่านั้น (Internal use)
- ส่วนบุคคล (Personal)
- เปิดเผยได้ (Public)

๑.๒ ผู้ใช้งานต้องพิจารณาองค์ประกอบต่อไปนี้เพื่อเป็นแนวทางกำหนดชั้นความลับของข้อมูล

(๑) ความสำคัญของเนื้อหา คือ เนื้อหาของข้อมูลนั้นมีความสำคัญต่อความสำเร็จของงานตามภารกิจของสำนักงาน ปปง. มากน้อยเพียงใด หากมีความสำคัญสูง ข้อมูลนั้นจะสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายในเท่านั้น หรือลับ เป็นต้น

(๒) แหล่งที่มาของข้อมูล คือ หากข้อมูลนั้นมาจากภายนอกและเป็นข้อมูลลับ ชั้นความลับจะต้องคงไว้เช่นเดิม หรือหากข้อมูลนั้นมาจากอินเทอร์เน็ต ชั้นความลับจะเป็นประเภทเปิดเผยได้ เป็นต้น

(๓) วิธีการนำไปใช้ประโยชน์ คือ หากข้อมูลนั้นสามารถนำไปใช้ประโยชน์ในเชิงพาณิชย์ได้ หากถูกเปิดเผยจะส่งผลกระทบด้านการดำเนินคดีของสำนักงาน ปปง. ดังนั้น ข้อมูลนี้จะอยู่ในประเภทชั้นความลับ เป็นต้น

(๔) จำนวนบุคคลที่ควรรับทราบ ได้แก่ หากข้อมูลนั้นสามารถเปิดเผยต่อผู้ใช้งานข้อมูลเป็นจำนวนมาก ชั้นความลับจะเป็นข้อมูลเปิดเผยได้ เป็นต้น

(๕) ผลกระทบหากมีการเปิดเผย คือ หากข้อมูลนั้นถูกเปิดเผย จะมีผลกระทบด้านชื่อเสียงและภาพลักษณ์ ด้านการดำเนินคดี ด้านการปฏิบัติตามกฎระเบียบข้อบังคับที่องค์กรต้องปฏิบัติตาม หรือด้านการมีส่วนได้ส่วนเสียของผู้ที่เกี่ยวข้อง ดังนั้น ข้อมูลสามารถจัดอยู่ในชั้นความลับประเภทใช้ภายใน หรือลับ เป็นต้น

(๖) หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่อง คือ ข้อมูลสำคัญหรือข้อมูลลับที่มาจากเจ้าของเรื่องใด จะต้องคงชั้นความลับไว้เช่นเดิม การนำไปใช้งานควรขออนุญาตจากผู้ที่เป็นเจ้าของเรื่องก่อน เป็นต้น

(๗) สำหรับข้อมูลในชั้นความลับ “ลับ” ได้แก่ ลับ ลับมาก หรือลับที่สุด โดยเจ้าของข้อมูลต้องพิจารณาเกณฑ์ต่อไปนี้เพิ่มเติมเพื่อกำหนดชั้นความลับที่ถูกต้อง

- ลับที่สุด หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐหรือหน่วยงานอย่างร้ายแรงที่สุด
- ลับมาก หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐ หรือหน่วยงานอย่างร้ายแรง
- ลับ หมายความถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อประโยชน์แห่งรัฐ หรือหน่วยงาน

(๘) การดำเนินการกับข้อมูลลับ (ถ้ามี) เจ้าของข้อมูลลับต้องจัดทำทะเบียนข้อมูลลับที่ตนเองดูแล หรือรับผิดชอบ ซึ่งมีรายการดังนี้

- ชื่อของข้อมูล
- ระดับชั้นความลับและระดับชั้นการเข้าถึง
- ชื่อเจ้าของข้อมูลลับ
- หน่วยงานภายในที่สามารถเข้าถึงได้
- หน่วยงานภายนอกที่อนุญาตให้เข้าถึงได้

- สถานที่จัดเก็บข้อมูล

- ช่องทางการเข้าถึง

- ระยะเวลาการเก็บรักษาข้อมูล

- ระยะเวลาที่ได้เข้าถึง

(๙) พิจารณาปรับชั้นความลับ (ปรับลด เพิ่ม หรือยกเลิกชั้นความลับ) ตามความจำเป็นปรับปรุงทะเบียนข้อมูลลับให้ถูกต้องและทันสมัยและต้องแจ้งให้หน่วยงานที่สามารถเข้าถึงข้อมูล หรือที่ได้รับการแจกจ่ายทราบด้วยทุกครั้ง เพื่อแก้ไขชั้นความลับให้ถูกต้อง

(๑๐) ในการจัดทำหรือจัดเตรียมข้อมูลลับให้ผู้ใช้งานปฏิบัติ ดังนี้

- จัดทำหรือจัดเตรียมข้อมูลในสถานที่ปลอดภัย ได้แก่ จัดทำภายในสำนักงาน ปปง. ไม่จัดทำในสถานที่สาธารณะซึ่งบุคคลภายนอกสามารถเห็นข้อมูลที่จัดทำได้และจำกัดบุคคลเฉพาะผู้ที่เกี่ยวข้องในการเข้าถึงข้อมูล

- ในการจัดทำข้อมูลลับซึ่งใช้กระดาษ หรือวัสดุชั่วคราว ได้แก่ กระดาษร่าง กระดาษคาร์บอน ต้องทำลายกระดาษ หรือวัสดุนั้นทันทีที่จัดทำเสร็จเรียบร้อย ถ้าเป็นการจัดทำโดยใช้เครื่องคอมพิวเตอร์ จะต้องลบหรือทำลายสื่อบันทึกข้อมูลจนไม่สามารถนำไปใช้ประโยชน์ได้ (ดูวิธีการทำลายในตารางแสดงแนวทางปฏิบัติในการทำลายข้อมูลบนสื่อบันทึกข้อมูลในข้อ (๑๖) ที่จะกล่าวต่อไป) หากไม่ทำลายต้องเก็บรักษาไว้ในสถานที่ที่ปลอดภัย

- จัดทำข้อมูลโดยแสดงเลขที่หน้าของจำนวนหน้าทั้งหมดไว้ในทุกหน้าของข้อมูลลับและแสดงไว้ในส่วนที่สามารถเห็นได้ชัดเจน ได้แก่ มุมขวาด้านบนของเอกสาร (การบันทึกเลขหน้ามีจุดประสงค์ เพื่อให้ทราบว่าข้อมูลลับนั้นเป็นหน้าใดของจำนวนทั้งหมด หากมีการสูญหายไปหน้าใดหน้าหนึ่งจะได้ทราบและสามารถติดตามหาผู้ละเมิดและหาทางลดหรือแก้ไขความเสียหายที่เกิดขึ้นได้)

(๑๑) ในการแสดงชั้นความลับบนข้อมูลลับ ให้ปฏิบัติดังนี้

- แสดงชั้นความลับของข้อมูล ซึ่งประกอบด้วย “ลับ” “ลับมาก” หรือ “ลับที่สุด” ให้ปรากฏเห็นอย่างเด่นชัดทั้งข้อมูลที่มีสภาพเป็นกระดาษ ไฟล์อิเล็กทรอนิกส์ เทป External Hard Disk, Flash Drive แผ่น CD/DVD หรือข้อมูลลับที่อยู่ในรูปแบบอื่นๆ

- แสดงชั้นความลับบนเอกสารลับในทุกหน้าของเอกสารให้ปรากฏเห็นอย่างเด่นชัด

(๑๒) ในการทำสำเนาหรือแจกจ่ายข้อมูลลับให้ปฏิบัติ ดังนี้

- ทำสำเนาหรือแจกจ่ายข้อมูลลับให้แก่ผู้รับปลายทาง ซึ่งเป็นผู้ที่มีสิทธิในการเข้าถึงข้อมูลตามที่ระบุไว้ในทะเบียนข้อมูลลับหรือสามารถแจกจ่ายให้ได้ตามความจำเป็นในการเข้าถึงข้อมูลนั้น

- แจ้งให้หน่วยงานภายนอกที่อนุญาตให้เข้าถึงข้อมูลลับนั้นได้ ว่าไม่อนุญาตให้ทำสำเนาเพิ่มเติม เว้นเสียแต่ได้รับอนุญาตจากผู้มีอำนาจลงนามอนุญาตก่อน

(๑๓) ในการเก็บรักษาเอกสารลับให้ปฏิบัติ ดังนี้

- จัดเก็บเอกสารลับไว้ในแฟ้มข้อมูลลับและนำไปเก็บไว้ในตู้เก็บเอกสารลับโดยแยกเก็บเป็นแต่ละเรื่อง หรือแต่ละหัวข้อ

- ไม่จัดเก็บเอกสารลับร่วมกับเอกสารที่อยู่ในชั้นความลับอื่นๆ ได้แก่ ข้อมูลใช้ภายในเท่านั้น ข้อมูลส่วนบุคคล หรือข้อมูลที่เปิดเผยได้

- จัดเก็บแฟ้มข้อมูลลับไว้ในตู้และปิดล็อคด้วยกุญแจที่แข็งแรงและมั่นคง

(๑๔) ในการยืมหรือขอเข้าถึงข้อมูลลับให้ปฏิบัติ ดังนี้

- เมื่อมีการขอยืมหรือขอเข้าถึงข้อมูลลับโดยผู้อื่นที่ไม่ได้เป็นผู้มีสิทธิในการเข้าถึงข้อมูลตามทะเบียนข้อมูลลับ ให้หัวหน้าของส่วนงานที่รับผิดชอบเป็นผู้พิจารณาตรวจสอบคุณสมบัติของผู้ยืมหรือขอเข้าถึงก่อน ว่าเป็นผู้มีอำนาจหน้าที่ที่เกี่ยวข้องหรือไม่ หรือมีความจำเป็นในการเข้าถึงข้อมูลนั้นหรือไม่พร้อมทั้งต้องทำบันทึกหลักฐานการยืมหรือการขอเข้าถึงข้อมูลนั้นด้วยและแจ้งให้ผู้ยืมหรือขอเข้าถึงทราบว่าห้ามทำสำเนาเพิ่มเติม

- เมื่อหมดความจำเป็นในการใช้งานแล้ว หัวหน้าของส่วนงานที่รับผิดชอบกำหนดให้ผู้ขอยืมจัดส่งข้อมูลนั้นกลับคืนมาโดยทันที สำหรับกรณีการเข้าถึงระบบสารสนเทศ ให้ยกเลิกบัญชีผู้ใช้งานที่ขอเข้าถึงข้อมูลลับโดยทันที

(๑๕) ในการส่งเอกสารลับทางจดหมายอิเล็กทรอนิกส์ (E-Mail) ให้ปฏิบัติตามระเบียบการส่งเอกสารลับของสำนักงาน ปปง. เพื่อตรวจสอบที่อยู่ E-Mail ของผู้รับปลายทางให้ถูกต้องก่อนจัดส่งไฟล์ข้อมูลนั้นไปยังผู้รับเพื่อป้องกันการส่งผิดตัวบุคคล

(๑๖) ในการทำลายข้อมูลลับ ให้ปฏิบัติตามมาตรฐาน NIST800-88 เพื่อทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ

(๑๗) ในการจัดการกับไฟล์ข้อมูลลับให้ปฏิบัติ ดังนี้

- จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ (E-File) ที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหากและป้องกันให้มีความปลอดภัยอย่างพอเพียงต่อการเข้าถึงและควรแสดงชั้นความลับบนไฟล์ข้อมูลลับ โดยการทำสัญลักษณ์ลายน้ำและแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

- การสำเนา E-File ที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล

- ระมัดระวังการเผยแพร่ หรือแจกจ่าย E-File ที่เป็นความลับของสำนักงาน ปปง. ไปยังกลุ่มผู้รับ ต้องเฉพาะกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

- ผู้เป็นเจ้าของ E-File ต้องตรวจสอบความถูกต้องของ E-File ก่อนนำไปใช้งาน

- ผู้เป็นเจ้าของ E-File ที่เป็นความลับ หรือที่มีระดับความสำคัญสูง จะต้องเข้ารหัสข้อมูล (Encryption) ด้วย Certification authority (CA), การเข้ารหัสแบบ RSA หรือวิธีการเข้ารหัสแบบอื่นที่ได้รับรองมาตรฐานสากล หรือตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดก่อนส่ง โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยการใช้รหัสผ่านที่มีความมั่นคงปลอดภัยและไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์

- ห้ามแบ่งปัน (Share) ไฟล์ข้อมูลลับบนเครือข่ายสาธารณะ (Internet) ของสำนักงาน ปปง. เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)

- ตรวจสอบการทำงานของระบบป้องกันไวรัสในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับอย่างสม่ำเสมอว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

- ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมสำนักงาน เพื่อแก้ไขช่องโหว่ของโปรแกรมในเครื่องตามปกติหรือไม่

- สำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอ หรือตามความจำเป็น

- ต้องทำลาย E-File บนหน่วยความจำหลัก (Hard disk) ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

หมวด ๔
แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

ข้อ ๑ การใช้เครื่องคอมพิวเตอร์ภายในสำนักงาน ปปง. ให้เจ้าหน้าที่ปฏิบัติ ดังต่อไปนี้

๑.๑ ห้ามใช้เครื่องคอมพิวเตอร์จนกว่าจะได้รับการอนุมัติให้ใช้งาน โดยให้กรอกข้อมูลขอใช้งานเครื่องคอมพิวเตอร์

๑.๒ การใช้งานเครื่องคอมพิวเตอร์ต้องตรวจสอบการทำงานของโปรแกรมป้องกันไวรัสและการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) ก่อนใช้งานทุกครั้ง หากพบว่าโปรแกรมดังกล่าวทำงานผิดปกติให้รีบแจ้งศูนย์เทคโนโลยีสารสนเทศ เพื่อดำเนินการแก้ไขโดยเร็ว

๑.๓ เครื่องคอมพิวเตอร์ที่ใช้ภายในสำนักงาน ปปง. ให้ติดตั้งโปรแกรมมาตรฐานตามที่ศูนย์เทคโนโลยีสารสนเทศกำหนดให้ห้ามเปลี่ยนแปลง หรือติดตั้งโปรแกรมเพิ่มเติม เว้นแต่จะได้รับความเห็นชอบจากหัวหน้าหน่วยงานภายในสำนักงาน ปปง. เท่านั้น

ความในข้อ ๑.๓ ดังกล่าว ไม่ใช้บังคับแก่การเปลี่ยนแปลงหรือการติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติม เพื่อทดลองการใช้งานซึ่งดำเนินการโดยศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับการว่าจ้างให้มาจัดทำ หรือดูแลระบบสารสนเทศของสำนักงาน ปปง.

๑.๔ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์เพื่อไม่ให้บุคคลภายนอกสามารถใช้งานเครื่องคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ของสำนักงาน ปปง. ได้

๑.๕ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกจากโปรแกรมตามมาตรฐานที่ศูนย์เทคโนโลยีสารสนเทศกำหนดให้

๑.๖ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ในทรัพย์สินทางปัญญาของบุคคลอื่น

๑.๗ ห้ามเปลี่ยนแปลงหรือแก้ไขซอฟท์แวร์ที่มีลิขสิทธิ์ถูกต้องของสำนักงาน ปปง.

๑.๘ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่ายคอมพิวเตอร์

๑.๙ ต้องระมัดระวังการใช้งานและดูแลเครื่องคอมพิวเตอร์ รวมทั้งระบบเครือข่ายตามที่วิญญูชนทั่วไปจะพึงปฏิบัติ

๑.๑๐ เอกสารหรือข้อมูลต่างๆ ไม่ว่าจะอยู่ในรูปแบบใดก็ตามที่ได้มีการกำหนดเงื่อนไขการใช้งานไว้ต้องใช้งานด้วยความระมัดระวังและต้องปฏิบัติตามเงื่อนไขอย่างเคร่งครัด เพื่อป้องกันมิให้เกิดการละเมิดตามกฎหมาย

๑.๑๑ ต้องลบข้อมูลที่ไม่จำเป็นต่อการใช้งานออกจากเครื่องคอมพิวเตอร์ เพื่อประหยัดปริมาณหน่วยความจำบนสื่อบันทึกข้อมูล

๑.๑๒ ต้องออกจากระบบ (Logout) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าคอมพิวเตอร์ รวมทั้งปิดเครื่องคอมพิวเตอร์เมื่อใช้งานประจำวันเสร็จสิ้น

๑.๑๓ การติดตั้งโปรแกรมเพิ่มเติม ต้องเป็นโปรแกรมที่มีลิขสิทธิ์และใช้ในการทำงานซึ่งต้องได้รับอนุญาตจากผู้มีอำนาจ

๑.๑๔ การนำเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่อื่นใดมาใช้กับระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน ปปง. ต้องได้รับการตรวจสอบและอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

ข้อ ๒ การใช้เครื่องคอมพิวเตอร์แบบพกพา (Notebook) ของสำนักงาน ปปง. นอกจากต้องปฏิบัติตามที่กำหนดไว้ในข้างต้นแล้ว ให้เจ้าหน้าที่ปฏิบัติดังต่อไปนี้

๒.๑ ต้องตรวจสอบเครื่องคอมพิวเตอร์แบบพกพาที่นำไปใช้ว่าได้ติดตั้งโปรแกรมคอมพิวเตอร์ตามมาตรฐานที่ศูนย์เทคโนโลยีสารสนเทศให้แล้วหรือไม่ หากพบว่ายังไม่ได้ติดตั้งให้แจ้งผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. เพื่อขอรับการติดตั้งก่อนการใช้งาน

๒.๒ ต้องระมัดระวังไม่ให้บุคคลภายนอกมองเห็น หรือคัดลอกข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาที่นำไปใช้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

๒.๓ เมื่อหมดความจำเป็นที่ต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาแล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ผู้รับผิดชอบทันที ทั้งนี้ให้เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมในการใช้งานของเครื่องคอมพิวเตอร์ที่รับคืนไว้ดังกล่าวด้วย

ข้อ ๓ ในกรณีที่เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนเครื่องคอมพิวเตอร์แบบพกพาตรวจพบความเสียหาย ให้แจ้งผู้บังคับบัญชาทราบโดยเร็ว และหากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทเลินเล่ออย่างร้ายแรงของผู้นำไปใช้ ต้องให้ผู้นำไปใช้รับผิดชอบต่อความเสียหายที่เกิดขึ้นดังกล่าว

ข้อ ๔ การใช้เครื่องคอมพิวเตอร์เพื่อประโยชน์ส่วนตัวของเจ้าหน้าที่ให้ใช้ได้ภายในสถานที่สำนักงาน ปปง. จัดไว้เป็นการเฉพาะเท่านั้น

ข้อ ๕ การเข้าถึงระบบสารสนเทศ เจ้าหน้าที่ใช้งานต้องปฏิบัติตามข้อกำหนด ดังนี้

๕.๑ กรอกแบบเพื่อขออนุมัติใช้งานระบบงานและนำเสนอต่อผู้บังคับบัญชาเพื่อขออนุมัติ

๕.๒ ต้องไม่เข้าถึงระบบงานอื่นที่ไม่ได้รับอนุญาตให้ใช้งาน

๕.๓ ต้องออกจากระบบงานโดยทันที เมื่อใช้งานเสร็จสิ้น

ข้อ ๖ การใช้งานอินเทอร์เน็ต ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

๖.๑ ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

- การพนัน
- การประมูล
- วิพากษ์วิจารณ์ที่เกี่ยวข้องกับชาติ ศาสนา และพระมหากษัตริย์
- ลามก อนาจาร
- อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม

๖.๒ ห้ามเล่นเกมส์ หรือดาวน์โหลดเกมส์ ภาพยนตร์ เพลง หรือสื่อลามกอนาจารผ่านทางอินเทอร์เน็ต

๖.๓ ห้ามใช้อินเทอร์เน็ตเพื่อเผยแพร่หรือแจกจ่าย ดังต่อไปนี้

- สื่อสิ่งพิมพ์อิเล็กทรอนิกส์ที่เป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของ
- ข้อมูลประเภทสื่อลามกอนาจาร
- ข้อมูลที่เป็นความลับของสำนักงาน ปปง. ไปยังบุคคลที่ไม่ได้รับอนุญาต
- ข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

๖.๔ ห้ามใช้งานข้อมูลที่ได้รับโดยผ่านทางอินเทอร์เน็ตที่มีลักษณะเป็นการละเมิดลิขสิทธิ์ของผู้เป็นเจ้าของข้อมูลนั้น

๖.๕ ห้ามใช้อินเทอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่ก่อให้เกิดความเสียหายต่อภาพลักษณ์หรือชื่อเสียงของสำนักงาน ปปง.

ข้อ ๗ การใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

๗.๑ ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ตามที่สำนักงาน ปปง. กำหนดเท่านั้น

๗.๒ ห้ามเข้าถึง E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต

๗.๓ ห้ามปลอมแปลง รับหรือส่ง E-mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต

๗.๔ ห้ามส่ง E-mail ที่มีลักษณะดังต่อไปนี้

- จดหมายขยะ (Spam Mail)
- จดหมายลูกโซ่ (Chain Letter)
- จดหมายที่ละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น
- จดหมายที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

๗.๕ ห้ามส่ง E-mail ที่มีขนาดใหญ่เกินกว่าที่กำหนด

๗.๖ ต้องกรอกชื่อเรื่อง (Subject) และชื่อผู้ส่งใน E-mail ทุกฉบับที่ส่งไป

๗.๗ ต้องใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับ E-mail เท่าที่มีความจำเป็นต้องรับรู้เท่านั้น

๗.๘ ต้องใช้คำที่สุภาพในการส่ง E-mail

๗.๙ ต้องสำรองข้อมูล E-mail Address ตามความจำเป็นอย่างสม่ำเสมอ

ข้อ ๘ ห้ามมิให้เจ้าหน้าที่เข้าใช้งานระบบสารสนเทศของสำนักงาน ปปง. กระทำการในลักษณะอย่างใดอย่างหนึ่งดังต่อไปนี้

๘.๑ กระทำผิดกฎหมายหรือก่อให้เกิดความเสียหายแก่บุคคลอื่นหรือขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน หรือละเมิดทรัพย์สินทางปัญญาของสำนักงาน ปปง. และของบุคคลอื่น

๘.๒ เปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงาน ทั้งที่เป็นข้อมูลของสำนักงาน ปปง. หรือบุคคลภายนอก

๘.๓ การเข้าถึงข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาต

๘.๔ ขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของสำนักงาน ปปง. หรือเจ้าหน้าที่คนอื่นของสำนักงาน ปปง.

๘.๕ แสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับสำนักงาน ปปง. ไปยังที่อยู่เว็บไซต์ใดๆ ในลักษณะที่ก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริงและก่อให้เกิดความเสียหายแก่สำนักงาน ปปง.

๘.๖ กระทำการอื่นใดที่อาจขัดต่อการดำเนินงานตามอำนาจหน้าที่ของสำนักงาน ปปง. หรืออาจก่อให้เกิดความขัดแย้ง หรือความเสียหายแก่สำนักงาน ปปง.

ข้อ ๙ เอกสารที่เป็นความลับ หรือมีระดับความสำคัญซึ่งพิมพ์ออกมาจากเครื่องพิมพ์ (Printer) เจ้าหน้าที่ต้องปฏิบัติให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับของทางราชการ ดังต่อไปนี้

๙.๑ จัดหมวดหมู่เอกสารที่เป็นความลับ หรือที่มีระดับความสำคัญสูงไว้ต่างหาก

๙.๒ จัดเก็บและกำหนดวิธีการป้องกันที่มีความปลอดภัยอย่างเพียงพอ

๙.๓ การสำเนาเอกสารที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูง ต้องได้รับอนุญาตจากผู้เป็นเจ้าของ

๙.๔ ระมัดระวังการเผยแพร่ หรือแจกจ่ายเอกสารที่เป็นความลับของสำนักงาน ปปง. ไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

๙.๕ ตรวจสอบความถูกต้องของเอกสารก่อนนำไปใช้งาน

๙.๖ ให้ทำลายเอกสารที่เป็นความลับ หรือมีระดับความสำคัญสูงเมื่อหมดความจำเป็นในการใช้งาน

ข้อ ๑๐. การจัดการข้อมูลที่เป็นความลับที่อยู่ในรูปอิเล็กทรอนิกส์ ผู้ใช้งานปฏิบัติตามแนวทางปฏิบัติในการจัดการกับข้อมูลลับในข้อข้างต้น

ข้อ ๑๑ ผู้ใช้งานควรตรวจสอบ E-mail ที่ได้รับทุกครั้ง ว่าเข้าข่ายลักษณะการเป็นจดหมายขยะ (Spam mail) หรือไม่ โดยผู้ใช้งานต้องปฏิบัติตามข้อกำหนด ดังนี้

๑๑.๑ ตรวจสอบแหล่งที่มาของ E-mail ก่อนเปิดอ่าน โดยให้สังเกตลักษณะของจดหมายขยะ (Spam mail) ดังนี้

- ชื่อผู้ส่งจะไม่สามารถค้นหาที่มาได้ และ/หรือเป็นชื่อที่ผู้ใช้งานไม่รู้จัก/ไม่คุ้นเคย
- ชื่อเรื่องของ E-mail จะเป็นข้อความที่โน้มน้าวให้น่าสนใจ เพื่อต้องการให้ผู้ใช้งานเปิดอ่าน

๑๑.๒ ตรวจสอบเนื้อหาของ E-mail โดยมีจุดสังเกต ดังนี้

- E-mail ที่ไม่มีเนื้อหา
- E-mail ที่มีเนื้อหาเกี่ยวกับการโฆษณาสินค้า ผลิตภัณฑ์ หรือบริการ

- E-mail ที่มีลักษณะหลอกลวงโดยสอบถามข้อมูลที่เป็นความลับ หรือข้อมูลที่ไม่ควรเปิดเผยสู่สาธารณะ

- E-mail ที่ใช้เนื้อหาในลักษณะของรูปภาพแทนตัวอักษร

- E-mail ที่แนบไฟล์ที่อาจเป็น Virus หรือ Trojan และมีเนื้อหาเชิญชวนให้ผู้ใช้งานดาวน์โหลดหรือ Run ไฟล์ดังกล่าว

ข้อ ๑๒ ในกรณีที่ผู้ใช้งานได้รับจดหมายขยะ (Spam mail) ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดดังนี้

๑๒.๑ ห้ามเปิดอ่าน E-mail ฉบับนั้นโดยเด็ดขาด และให้แจ้งเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ ทราบทันที

๑๒.๒ ในกรณีที่เปิดอ่านแล้ว ห้ามคลิกที่ Link ข้อมูล หรือดาวน์โหลดไฟล์ที่แนบมากับ E-mail ฉบับนั้น และให้แจ้งเจ้าหน้าที่ศูนย์เทคโนโลยีและสารสนเทศทราบทันที

หมวด ๕

แนวปฏิบัติและหน้าที่ของผู้ดูแลระบบสารสนเทศ /ผู้ดูแลระบบเครือข่าย

ข้อ ๑ ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศ ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) และระบบเครือข่ายของสำนักงาน ปปง. ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจเกิดขึ้นในทันทีและในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นกับสำนักงาน ปปง. ให้ผู้ดูแลระบบ (System Administrator) พิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้งานดังกล่าวได้ทันที

ข้อ ๒ ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

ข้อ ๓ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server) ระบบสารสนเทศ และระบบเครือข่าย

ข้อ ๔ ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอและปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

ข้อ ๕ บริหารจัดการบัญชีผู้ใช้งานและควบคุมการเข้าถึงตามอำนาจหน้าที่เท่านั้น

ข้อ ๖ บริหารจัดการระบบสารสนเทศและระบบเครือข่ายตามอำนาจหน้าที่รับผิดชอบเท่านั้น

ข้อ ๗ บริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตามอำนาจหน้าที่รับผิดชอบเท่านั้น

ข้อ ๘ ไม่ใช้อำนาจหน้าที่ของตนเองในการเข้าถึงข้อมูลของผู้ใช้งานบนระบบคอมพิวเตอร์ระบบสารสนเทศและระบบเครือข่าย โดยไม่มีเหตุผลอันสมควร

ข้อ ๙ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้งานเครื่องคอมพิวเตอร์ ระบบสารสนเทศและระบบเครือข่าย โดยไม่มีเหตุผลอันสมควร

ข้อ ๑๐ ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่สามารถเปิดเผยได้ให้บุคคลอื่นทราบ โดยไม่มีเหตุผลอันสมควร

ข้อ ๑๑ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็น เพื่อให้สามารถระบุตัวตนผู้ใช้งานและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วัน นับจากการใช้บริการสิ้นสุดลง

ข้อ ๑๒ กำหนดและปรับปรุงระดับการคัดกรองจดหมาย (E-mail Filtering) ของเครื่องคอมพิวเตอร์แม่ข่าย (Mail server) ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

หมวด ๖
แนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยระบบเครือข่าย

ข้อ ๑ กำหนดมาตรการทางเครือข่ายและการสื่อสารข้อมูลเพื่อป้องกันข้อมูลในเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศ หรือบริการต่างๆ จากการถูกเข้าถึงหรือถูกทำลายโดยไม่ได้รับอนุญาต ดังต่อไปนี้

๑.๑ กำหนดบุคลากรผู้มีหน้าที่รับผิดชอบ ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่ใช้ในการเข้าถึงจากระยะไกล ให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (Virtual Private Network : VPN) โดยมีการเข้ารหัสรักษาความปลอดภัยแบบ Secure Sockets Layer (SSL) หรือ Secure Shell (SSH) หรือเทียบเท่า

๑.๒ กำหนดมาตรการพิเศษเพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญเมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ ได้แก่ เครือข่ายอินเทอร์เน็ต เครือข่ายไร้สาย เป็นต้น

๑.๓ การเข้าสู่ระบบสารสนเทศภายในองค์กร สำหรับผู้ใช้นอกองค์กร (Guest, Teleworking) ต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง ด้วยการใช้รหัสผ่าน หรือโทเคน หรือใช้ร่วมกัน โดยจะต้องลงทะเบียนและขอรับได้ที่ศูนย์เทคโนโลยีสารสนเทศ

๑.๔ กำหนดข้อปฏิบัติในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์พกพาและโทรศัพท์มือถือ ต้องมีการยืนยันตัวตนในการเข้าใช้งานทุกครั้งด้วยการใช้รหัสผ่านที่ออกให้โดยศูนย์เทคโนโลยีสารสนเทศ ซึ่งสิทธิที่ได้จะแตกต่างและมีข้อกำหนดการใช้งานที่จำกัด

๑.๕ มีการบันทึกข้อมูลพฤติกรรมการใช้งานเก็บ Log ของอุปกรณ์เครือข่าย เพื่อใช้ในการตรวจสอบอย่างสม่ำเสมอ

ข้อ ๒ ผู้รับผิดชอบหรือผู้ดูแลระบบสารสนเทศ ภายในสำนักงาน ปปง. จะต้องปฏิบัติตามข้อกำหนดดังต่อไปนี้

๒.๑ ผู้ดูแลระบบต้องออกแบบการแบ่งระบบเครือข่าย (Segregation in Networks) ตามกลุ่มของบริการระบบสารสนเทศ และการสื่อสารที่มีการใช้งาน ดังนี้

(๑) Internal สำหรับสินทรัพย์และระบบสารสนเทศให้หรือใช้บริการเฉพาะภายในสำนักงาน ซึ่งมีความไวต่อการรบกวน มีผลกระทบและความสำคัญสูง

(๒) Intranet สำหรับสินทรัพย์และระบบสารสนเทศให้หรือใช้บริการเฉพาะภายในสำนักงาน

(๓) Extranet สำหรับสินทรัพย์และระบบสารสนเทศให้หรือใช้บริการเฉพาะระหว่างองค์กรภายนอก โดยต้องมีมาตรการกำกับดูแลเข้มงวดสูงกว่าโซน Intranet

(๔) VPN สำหรับการเข้าใช้สินทรัพย์และระบบสารสนเทศสำนักงานจากภายนอก (Teleworking) โดยต้องมีมาตรการกำกับดูแลเข้มงวดสูงกว่าโซน Intranet

(๕) Wireless สำหรับเครือข่ายไร้สาย และอุปกรณ์เคลื่อนที่ โดยต้องมีมาตรการกำกับดูแลเข้มงวดสูงกว่าโซน Intranet

(๖) DMZ สำหรับส่วนให้หรือใช้บริการสาธารณะเครือข่ายอินเทอร์เน็ต โดยต้องมีมาตรการกำกับดูแลเข้มงวดสูงสุดเพื่อเป็นการควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๒.๒ การเข้าสู่ระบบเครือข่ายภายในสำนักงาน ปปง. โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาก่อนที่จะสามารถใช้งานได้ในทุกกรณี

๒.๓ ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายและระบบสารสนเทศ ที่ได้รับอนุญาตให้เข้าถึงเท่านั้น โดยมีระบบสารสนเทศที่จำเป็นต้องมีการควบคุมการเข้าถึง

๒.๔ ผู้ดูแลระบบจะต้องตรวจสอบและจำกัดเส้นทางการเข้าถึงเครือข่าย โดยการปิดเส้นทางของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นออกจากระบบ

๒.๕ ผู้ดูแลระบบจัดให้มีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ ได้แก่ การใช้ MAC address หรือเทียบเท่าและวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ใช้งานไปยังเครื่องคอมพิวเตอร์ให้บริการ

๒.๖ ผู้ดูแลระบบมีการควบคุมและจัดเส้นทางบนเครือข่าย (network routing control) ที่เหมาะสมระหว่างหน่วยงานหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๒.๗ กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ต่างๆ ของระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์อย่างชัดเจนและมีการทบทวนการกำหนดค่าตัวแปร (Parameter) ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๒.๘ ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสำนักงาน ปปง. จะต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมป้องกันการบุกรุกในการทำ Packet filtering เป็นต้น

๒.๙ มีการติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายภายในสำนักงาน ปปง. ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๒.๑๐ การเข้าสู่ระบบงานเครือข่ายภายในสำนักงาน ปปง. ผ่านทางอินเทอร์เน็ต ต้องมีการพิสูจน์ตัวตน (Authentication) โดยการกรอกชื่อบัญชีผู้ใช้งาน (User Account) และรหัสผ่าน (Password) หรือเทียบเท่า สำหรับ Login เพื่อตรวจสอบความถูกต้อง

๒.๑๑ ข้อมูลหมายเลขชุดภายในของเครื่องคอมพิวเตอร์ (Local IP Address) ของระบบงานเครือข่ายภายในสำนักงาน ปปง. จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของสำนักงาน ปปง. ได้โดยง่าย

๒.๑๒ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๑๓ การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชาหรือผู้รับมอบอำนาจ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒.๑๔ ผู้ดูแลระบบกำหนดอุปกรณ์บนเครือข่ายเป็น VLAN และ Subnet แยกตามกลุ่มแต่ละสิทธิของผู้ใช้งาน โดยให้ควบคุมการใช้งานอย่างเหมาะสมและมีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

๒.๑๕ การบริหารจัดการการบันทึกและตรวจสอบ กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบ

๒.๑๖ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๒.๑๗ ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพ โดยปิดล็อกตู้เก็บอุปกรณ์และทางเครือข่าย โดยแยกเชื่อมเครือข่ายเป็นการเฉพาะ ซึ่งไม่สามารถเข้าถึงได้โดยเครือข่ายอื่นใด

ข้อ ๓ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless) ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องกำหนดแนวปฏิบัติตามข้อกำหนด ดังต่อไปนี้

๓.๑ ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในสำนักงาน ปปง. จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาก่อนการใช้งาน

๓.๒ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบ (Login) เครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

๓.๓ ผู้ดูแลระบบควรใช้ Software หรือ Hardware ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

หมวด ๗

แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการของผู้ใช้งาน

ข้อ ๑ ผู้ใช้งานจะต้องยืนยันการเข้าใช้งานโดยใช้ ชื่อบัญชีผู้ใช้งาน (User Account) และรหัสผ่าน (Password) หรือการยืนยันตัวตนผ่านระบบที่เป็นศูนย์กลาง (Active Directory) ก่อนเข้าใช้งานระบบปฏิบัติการเครื่องคอมพิวเตอร์ทุกครั้ง

ข้อ ๒ ผู้ใช้งานต้องไม่อนุญาตให้บุคคลอื่นใช้ ชื่อบัญชีผู้ใช้งาน (User Account) ของตนเองในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

ข้อ ๓ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมเพื่อล็อคหน้าจอโดยอัตโนมัติ หลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๕ นาที

ข้อ ๔ ผู้ใช้งานควรทำการลงบันทึกออก (Logout) ทุกครั้งที่มิได้ปฏิบัติงานอยู่หน้าเครื่องคอมพิวเตอร์ รวมทั้งปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเลิกใช้งาน

ข้อ ๕ ผู้ใช้งานต้องไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) รวมถึงโปรแกรมอรรถประโยชน์ใดๆ ที่อาจละเมิดหรือทำให้หลีกเลี่ยงมาตรการความมั่นคงปลอดภัยได้

ข้อ ๖ ผู้ใช้งานต้องกำหนดให้รหัสผ่านมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวเลข (Numerical Character) ตัวอักษร (Alphabet) และตัวอักขระพิเศษ (Special Character)

โดยไม่เป็นวันเดือนปี คำข้อความใดที่ง่ายต่อการล่วงรู้ หรือง่ายต่อการคาดเดา ทั้งนี้ ระบบที่เป็นศูนย์กลาง (Active Directory) จะมีการควบคุมการเปลี่ยนรหัสผ่านทุก ๖ เดือน และตรวจสอบการตั้งรหัสผ่านซ้ำ

หมวด ๘
แนวปฏิบัติในการสำรองข้อมูลสำคัญและการเตรียมรับมือกับเหตุฉุกเฉิน

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. เป็นผู้พิจารณาคัดเลือกระบบสารสนเทศเพื่อจัดทำระบบสำรอง นำส่งแผนสำรองข้อมูล อีกทั้งต้องใช้แนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล เมื่อมีระบบงานใหม่ เกิดข้อมูลใหม่ หรือข้อมูลที่มีการเปลี่ยนแปลงใหม่ ควรกำหนดให้ใช้แนวทางการสำรองและกู้คืนข้อมูล ที่เหมาะสม ดังนี้

๑.๑ ระบุระบบงานที่มีความจำเป็นต้องสำรองข้อมูลไว้

๑.๒ ระบุผู้รับผิดชอบในการสำรองข้อมูลและกรณีเกิดเหตุฉุกเฉิน

๑.๓ ระบุชนิดของข้อมูลที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้อย่างน้อยต้องประกอบด้วย ข้อมูลในฐานข้อมูลของระบบ ข้อมูลสำหรับตัวระบบ ได้แก่ โปรแกรมระบบปฏิบัติการ (Operation Software) และโปรแกรมอื่นๆ ที่เกี่ยวข้อง

๑.๔ ระบุความถี่ในการสำรองข้อมูลของระบบงาน ได้แก่ ระบบงานที่มีการเปลี่ยนแปลงบ่อยควรมีความถี่ในการสำรองข้อมูลไม่ต่ำกว่าสัปดาห์ละครั้ง ระบบงานทั่วควรมีความถี่ในการสำรองข้อมูลไม่ต่ำกว่าเดือนละครั้ง เป็นต้น

๑.๕ ระบุขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง รวมทั้งโปรแกรมที่ใช้ในการสำรองข้อมูล

๑.๖ ทำการสำรองข้อมูลตามความถี่ที่กำหนดไว้ และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

๑.๗ ทำการตรวจสอบว่าการสำรองที่เกิดขึ้นนั้น สำเร็จครบถ้วนหรือไม่

๑.๘ ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้และสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง รวมทั้งดำเนินการทดสอบว่าระบบงานทั้งหมดสามารถใช้งานได้หรือไม่

๑.๙ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยแผนฯ ควรมีรายละเอียดอย่างน้อยดังต่อไปนี้

(๑) การมอบหมายหน้าที่ และความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด ให้ชัดเจนที่สามารถเชื่อมโยงถึงตัวของบุคลากร ในเรื่องต่อไปนี้ ระบบสารสนเทศ ระบบสำรองและการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

(๒) การประเมินความเสี่ยงสำหรับระบบงานที่มีความสำคัญเหล่านั้นและวางมาตรการเพื่อลดความเสี่ยงเหล่านั้น ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) การระบุขั้นตอนปฏิบัติในการกู้คืนระบบงาน

(๔) การระบุขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) การระบุช่องทางในการติดต่อสื่อสารกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการเครื่องคอมพิวเตอร์ โปรแกรมและระบบเครือข่าย เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อในกรณีเกิดเหตุฉุกเฉินต่างๆ ไม่ว่า เกิดอัคคีภัย การก่อวินาศกรรม เป็นต้น

๑.๑๐ ให้ทำการปรับปรุงแผนฯ ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๑.๑๑ ให้จัดประชุม หรือสัมมนาและแจ้งให้ผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนฯ รวมทั้งเมื่อมีการปรับปรุงแผนใหม่จะต้องจัดประชุมใหม่และแจ้งให้ผู้ที่เกี่ยวข้องทราบเช่นเดียวกัน

หมวด ๙
แนวปฏิบัติในการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ ๑ การแจ้งเหตุการณ์ทางด้านความมั่นคงปลอดภัย

๑.๑ ให้เจ้าหน้าที่หรือผู้ปฏิบัติงานแจ้งไปยังศูนย์เทคโนโลยีสารสนเทศทันทีที่พบเห็นเหตุการณ์ที่อาจเป็นปัญหาต่อความมั่นคงปลอดภัยในการใช้ระบบสารสนเทศของสำนักงาน ปปง. ได้แก่

- มีโปรแกรมสำนักงานไม่ประสงค์ดีเข้ามาในระบบคอมพิวเตอร์
- มีการบุกรุกเข้ามาในระบบเครือข่าย
- ข้อมูลสำคัญเปลี่ยนแปลง หรือสูญหาย
- มีการเปิดเผยข้อมูลสำคัญโดยไม่ได้รับอนุญาต
- มีการนำข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์
- มีการใช้ระบบสารสนเทศ ผิดวัตถุประสงค์
- พบจุดอ่อนในเครื่องคอมพิวเตอร์ โปรแกรมและระบบเครือข่ายที่ใช้งาน
- มีการโจมตีเข้ามาในระบบจนไม่สามารถให้บริการได้
- ระบบสารสนเทศ ชำรุดหรือสูญหาย
- บุคคลภายนอกเข้าใช้ระบบงานของสำนักงาน ปปง. โดยไม่ได้รับอนุญาต
- มีการติดตั้งโปรแกรมเพื่อขโมยข้อมูลหรือเข้าถึงข้อมูลในระบบเครือข่าย
- เหตุการณ์อื่นๆ ที่เป็นการละเมิดความมั่นคงปลอดภัยของสำนักงาน ปปง.

๑.๒ ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชาหรือศูนย์เทคโนโลยีสารสนเทศ ในการตรวจสอบเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นรวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชาหรือศูนย์เทคโนโลยีสารสนเทศ ด้วย

ข้อ ๒ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. เมื่อได้รับแจ้งจากผู้ใช้งานเกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้นหรือที่พบ ให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

๒.๑ ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้นว่ามีผลกระทบในระดับใด (สูง กลาง หรือต่ำ)

๒.๒ แจ้งให้ผู้บังคับบัญชาตามลำดับชั้นได้รับทราบตามระดับของผลกระทบ กล่าวคือ รายงานไปสู่ระดับชั้นของผู้บังคับบัญชาที่สูงขึ้น ตามลำดับสำหรับเหตุการณ์ที่มีผลกระทบสูงกว่า

๒.๓ วิเคราะห์และแก้ไขสถานการณ์ตามความจำเป็นกรณีการบุกรุก การโจมตีระบบหรือระบบได้รับความเสียหาย ประสานงานขอความช่วยเหลือจากหน่วยงานที่รับผิดชอบหรือมีหน้าที่เกี่ยวข้อง ได้แก่ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) สกอช.

๒.๔ กรณีมีความจำเป็นต้องเก็บหลักฐานทางคอมพิวเตอร์ ให้ผู้ที่ผ่านการอบรมหรือฝึกฝนเป็นผู้ดำเนินการเพื่อป้องกันไม่ให้หลักฐานเกิดความเสียหาย จัดเก็บหลักฐานไว้ในสถานที่ที่ปลอดภัยและจำกัดการเข้าถึงหลักฐานนั้น

๒.๕ จัดทำรายงานสรุปเหตุการณ์นับตั้งแต่ได้รับแจ้งเฉพาะเหตุการณ์ที่มีผลกระทบตั้งแต่ระดับปานกลาง ขึ้นไปและแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ โดยมีข้อมูลอย่างน้อยในรายงาน ดังนี้

- รายละเอียดเหตุการณ์
- วันเวลาที่เกิดขึ้น
- ชื่อผู้แจ้ง/หน่วยงานผู้แจ้ง
- สถานะของเหตุการณ์ในแต่ละช่วงเวลา
- ความคืบหน้าในการดำเนินการในแต่ละช่วงเวลา
- สาเหตุและวิธีการแก้ไข
- ข้อเสนอแนะเพื่อป้องกันการเกิดซ้ำ

ข้อ ๓ ความรับผิดชอบของผู้บังคับบัญชากรณีที่มีการละเมิดการปฏิบัตินี้

๓.๑ ให้แจ้งรายงานตามสายการบังคับบัญชาให้หน่วยที่เกี่ยวข้องทราบ

๓.๒ สั่งการสอบสวนหาตัวผู้กระทำผิดและผู้รับผิดชอบโดยเร็วที่สุด

๓.๓ พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนี้อุบัติซ้ำอีก

๓.๔ ให้พิจารณาการลงโทษทางวินัยตามกฎหมายต่อผู้ละเมิด ผู้เกี่ยวข้องกับการละเมิดและผู้รับผิดชอบเมื่อมีการละเมิด หรือไม่ปฏิบัติตามระเบียบนี้โดยเจตนาหรือไม่เจตนาและการละเมิดนั้นก่อให้เกิดความเสียหาย หรือยังไม่เกิดความเสียหายต่อทางราชการก็ตาม

ข้อ ๔ ความรับผิดชอบของหน่วยงานที่รับผิดชอบระบบสารสนเทศ เมื่อได้รับแจ้งว่าได้เกิดการละเมิดการรักษาความปลอดภัยให้ส่วนราชการเจ้าของระบบสารสนเทศ ดำเนินการ ดังนี้

๔.๑ พิจารณาว่าข้อมูลสารสนเทศ เอกสารกรรมวิธีข้อมูลต่างๆ ประมวลลับหรือรหัสผ่านที่จำเป็นในการใช้เครือข่ายสื่อสารข้อมูลสารสนเทศมีผลกระทบกระเทือนเสียหายอย่างใดหรือไม่

๔.๒ ขจัดความเสียหายที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นจากการละเมิดโดยทันที ในการนี้อาจจะต้องดำเนินการแก้ไขเปลี่ยนแปลงแผนงานและวิธีปฏิบัติพร้อมทั้งปัจจัยต่างๆ ที่เกี่ยวข้องตามที่เห็นสมควร

ข้อ ๕ ความรับผิดชอบของผู้ใช้งานต่อประกาศฉบับนี้มี ดังนี้

๕.๑ ปฏิบัติตามประกาศนี้อย่างเคร่งครัดและต้องไม่ละเลยต่อหน้าที่ความรับผิดชอบของตนเอง

๕.๒ ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข หรือทำลายโดยไม่ได้รับอนุญาต หรือทำให้เสียหายต่อระบบคอมพิวเตอร์และเครือข่ายของสำนักงาน ปปง.

๕.๓ ไม่รบกวนหรือแทรกแซงการสื่อสารข้อมูลในเครือข่ายของสำนักงาน ปปง.

๕.๔ รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่พบไปยังสำนักงาน ปปง. โดยเร็วที่สุด

ข้อ ๖ มีการควบคุมสินทรัพย์ด้านสารสนเทศต่อการเข้าถึงต้องได้รับการอนุญาตโดยปฏิบัติดังนี้

๖.๑ กำหนดมาตรการป้องกันทรัพย์สินขององค์กร โดยรวบรวมสินทรัพย์ทั้งหมดไว้อย่างเป็นระบบ

๖.๒ เมื่อใช้งานระบบเสร็จ ต้องออกจากระบบทันที

๖.๓ ป้องกันไม่ให้ผู้ที่ไม่เกี่ยวข้องใช้อุปกรณ์ด้านสารสนเทศโดยไม่ได้รับอนุญาต

๖.๔ นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

หมวด ๑๐
แนวปฏิบัติในการจัดซื้อจัดจ้างระบบสารสนเทศ

ข้อ ๑ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องควบคุมการพัฒนาหรือจัดหาระบบงานเพื่อให้ระบบงานที่ได้รับมีความมั่นคงปลอดภัย ดังนี้

๑.๑ ให้ประเมินความเสี่ยงและระบุข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Requirements) ของระบบงานที่จะจัดหาหรือพัฒนาอย่างเป็นลายลักษณ์อักษร ข้อกำหนดดังกล่าวอย่างน้อยควรมีคุณสมบัติของการเข้าสู่ระบบงาน (Login) ที่มีความมั่นคงปลอดภัย ดังนี้

(๑) ไม่มีหรือไม่แสดงรูปแบบการใช้งาน (Function) ให้การช่วยเหลือในระหว่างที่เข้าสู่ระบบ (Login)

(๒) บันทึกความพยายามในการล็อกอินทั้งที่สำเร็จและไม่สำเร็จและแสดงประวัติการเข้าใช้ระบบ ๓ ครั้งล่าสุด

(๓) ตัดการเชื่อมต่อหลังจากที่ทำการเข้าใช้ระบบ ไม่สำเร็จเกินกว่า ๓ ครั้ง

(๔) เมื่อกรอกข้อมูลบัญชีชื่อผู้ใช้งานและรหัสผ่านที่ไม่ถูกต้อง ให้แสดงข้อความปรากฏว่า "ข้อมูลการ Login ไม่ถูกต้อง" หรือข้อความที่ให้ความหมายเดียวกัน

(๕) ให้แสดงข้อความเตือนที่หน้าจอภายหลังจากการเข้าสู่ระบบ (Login) เสร็จสิ้น ข้อความเตือนดังกล่าว ได้แก่ "ระบบนี้เป็นระบบที่เป็นทรัพย์สินของสำนักงาน ปปง. การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้น จึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงานหากมีการตรวจพบและเป็นความผิดจะดำเนินการลงโทษทางวินัย หรือดำเนินการทางกฎหมายตามความเหมาะสม สิทธิในการตรวจสอบพฤติกรรมการใช้งานในระหว่างที่ผู้ใช้งานใช้ระบบงานนี้โดยไม่ถือว่าเป็นการละเมิดความเป็นส่วนตัว"

(๖) ไม่แสดงรายละเอียดของระบบใดๆ จนกว่าจะเข้าสู่ระบบ (Login) สำเร็จ

(๗) การกำหนดหรือตั้งรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับเข้าถึงระบบงาน

(๘) การเข้ารหัสข้อมูลสำคัญที่มีการรับส่งระหว่างเครื่องคอมพิวเตอร์ลูกข่ายกับเครื่องคอมพิวเตอร์ที่ให้บริการ

(๙) การเข้ารหัสข้อมูลสำคัญ ได้แก่ ข้อมูลลับ ที่จัดเก็บไว้ในฐานข้อมูล

(๑๐) การตัดและหมดเวลาการใช้งานหลังจากที่ไม่ได้ใช้ระบบงานเกินกว่าระยะเวลาตามที่กำหนดไว้ ในช่วง ๑๕ - ๓๐ นาที สำหรับระบบทั่วไป และในช่วง ๕ - ๑๐ นาที สำหรับระบบที่มีความเสี่ยงหรือมีความสำคัญสูง

(๑๑) การบันทึกบัญชีชื่อผู้ใช้งานที่เข้าสู่ระบบ (Login) หมายเลข IP Address วันเวลาที่เข้าใช้ระบบสำเร็จ หรือไม่สำเร็จ ของผู้ใช้งาน

๑.๒ พัฒนาหรือจัดหาระบบงานให้ได้ตามข้อกำหนดทางด้านความมั่นคงปลอดภัยที่ระบุไว้

๑.๓ พัฒนาหรือจัดหาระบบงานเพื่อให้มีหน้าจอสำหรับผู้ดูแลระบบเพื่อทำการบันทึกและปรับปรุงสิทธิของผู้ใช้งานได้ รวมทั้งต้องสามารถบันทึกสิทธิดังกล่าวลงเก็บไว้ในฐานข้อมูลได้ด้วย

๑.๔ กำหนดให้มีการจัดทำแผนการทดสอบโดยผู้พัฒนาระบบ นำเสนอแผนฯ ดังกล่าวเพื่อพิจารณาอนุมัติโดยผู้มีอำนาจ ดำเนินการทดสอบตามแผนฯ บันทึกผลการทดสอบ และรายงานผลการ

ทดสอบ ให้ผู้มีอำนาจได้รับทราบเพื่อให้คำแนะนำในการปรับปรุงต่างๆ ที่จำเป็นแผนการทดสอบที่จัดทำอย่างน้อยประกอบด้วย

- แผนการทดสอบ UAT (User Acceptance Test)
- แผนการทดสอบ System Integration Test
- แผนการทดสอบข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Test)

๑.๕ ไม่อนุญาตการนำข้อมูลสำคัญของสำนักงาน ปปง. ไปใช้ในการทดสอบกับระบบงานเพื่อป้องกันการรั่วไหลของข้อมูล เว้นเสียแต่ได้รับการอนุมัติจากผู้บังคับบัญชาระดับสูงก่อน และหากเป็นไปได้ให้ตัดข้อมูลส่วนที่สำคัญทิ้งไป ให้เหลือเฉพาะส่วนที่เพียงพอต่อการนำไปใช้ในการทดสอบ

ข้อ ๒ ภายหลังจากที่ได้มีการตรวจรับระบบที่พัฒนาขึ้นใหม่แล้ว ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องกำหนดการควบคุมการติดตั้งโปรแกรมลงไปยังระบบเครื่องคอมพิวเตอร์ที่ให้บริการดังนี้

๒.๑ ให้มีการควบคุมการเปลี่ยนแปลงระบบงานภายในสำนักงาน ปปง. เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

๒.๒ ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงระบบงานภายในสำนักงาน ปปง.

๒.๓ การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

๒.๔ กำหนดให้มีการจัดเก็บรหัสโปรแกรม (Source Code) และบรรณานุกรมคำศัพท์ (Library) สำหรับโปรแกรมของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๒.๕ กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน ได้แก่ โปรแกรมระบบปฏิบัติการ โปรแกรมระบบงาน เป็นต้น

๒.๖ ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบงาน

๒.๗ ทำการปรับปรุง Library สำหรับโปรแกรมระบบงาน ให้มีความทันสมัยและสอดคล้องกับระบบทั้งหมดที่ทำการติดตั้ง

๒.๘ ในกรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิมให้ทำการสำรองข้อมูลที่จำเป็น ได้แก่ ฐานข้อมูล โปรแกรม ค่าปรับแต่งและติดตั้งระบบ หรืออื่นๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จจะได้สามารถถอยหลังกลับไปใช้ระบบงานเดิมได้

๒.๙ ในกรณีที่มีความจำเป็นต้องแปลงข้อมูลในระบบงานเดิมไปสู่ข้อมูลในระบบงานที่ทำการติดตั้ง ให้กำหนดแผนการถ่ายโอนหรือแปลงข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ให้ถ่ายโอนข้อมูลตามแผนฯ และร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

๒.๑๐ ให้กำหนดแผนการติดตั้งสำหรับระบบงานซึ่งรวมถึงระยะเวลาที่จะดำเนินการ รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า ได้แก่ แผนการติดตั้งเครื่องคอมพิวเตอร์ โปรแกรม ระบบเครือข่าย และอื่น ๆ

๒.๑๑ สำหรับโปรแกรมที่จะทำการติดตั้ง ให้ตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตโปรแกรมนั้น

๒.๑๒ ให้อ่านและปฏิบัติตามเงื่อนไขหรือข้อตกลงการใช้งานโปรแกรมที่จะทำการติดตั้งอย่างเคร่งครัด

๒.๑๓ สำหรับการติดตั้งโปรแกรมอเนกประสงค์ (Utility Software) ต้องตรวจสอบก่อนว่าเป็นโปรแกรมที่มีการทำงานที่ถูกต้องและเชื่อถือได้

๒.๑๔ ติดตั้งโปรแกรมสำนักงานแก้ไขช่องโหว่ (Patch) ที่เกี่ยวข้องกับระบบงาน ตามความจำเป็น ได้แก่ โปรแกรมสำนักงานแก้ไขช่องโหว่สำหรับระบบปฏิบัติการ โปรแกรมสำนักงานแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

๒.๑๕ ตรวจสอบและปิดพอร์ต (Port) บนระบบงานที่ไม่มีความจำเป็นในการใช้งานก่อนเปิดระบบให้บริการ

๒.๑๖ จัดให้มีการป้องกันไวรัสคอมพิวเตอร์บนระบบงานที่ทำการติดตั้ง

ข้อ ๓ ผู้รับผิดชอบระบบสารสนเทศของสำนักงาน ปปง. ต้องกำหนดให้มีการทบทวนการทำงานของระบบงานภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating System Changes) ดังนี้

๓.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๓.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบงาน รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่สำนักงาน ปปง. ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

ข้อ ๔ การดำเนินงานของบประมาณที่เกี่ยวข้องกับระบบสารสนเทศ หรือวัสดุอุปกรณ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ ต้องผ่านการพิจารณากลั่นกรองความเหมาะสมเบื้องต้นจากศูนย์เทคโนโลยีสารสนเทศ และนำเสนอคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์สำนักงาน ปปง. ให้ความเห็นชอบ

โดยผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำสำนักงาน ปปง. เป็นผู้พิจารณารับรองก่อนจะพิจารณาในขั้นตอนต่อไป

หมวด ๑๑
แนวปฏิบัติในการเผยแพร่ข้อมูลต่อสาธารณะ

ข้อ ๑ การเผยแพร่ข้อมูลในความรับผิดชอบของสำนักงาน ปปง. ต่อสาธารณะโดยผ่านระบบสารสนเทศของสำนักงาน ปปง. หน่วยงานเจ้าของข้อมูลจะต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำออกเผยแพร่ และหากข้อมูลที่นำออกเผยแพร่เกี่ยวข้องกับเรื่องนโยบายจะต้องได้รับความเห็นชอบจากเลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงินหรือผู้ซึ่ง เลขาธิการฯ มอบหมายก่อนนำออกเผยแพร่ ในกรณีที่ข้อมูลที่นำออกเผยแพร่มีความผิดพลาด และมีความเสียหายเกิดขึ้น โดยความเสียหายนั้นเกิดจากความจงใจหรือประมาทเลินเล่ออย่างร้ายแรง ให้เป็นความรับผิดชอบของเจ้าหน้าที่ผู้นำข้อมูลดังกล่าวออกเผยแพร่

ข้อ ๒ การเผยแพร่ข้อมูลต่อสาธารณะโดยผ่านระบบสารสนเทศของสำนักงาน ปปง. ให้ดำเนินการโดยหน่วยงานเจ้าของข้อมูล เว้นแต่กรณีที่เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน หรือผู้ซึ่ง เลขาธิการฯ มอบหมาย ได้สั่งการ หรือเห็นชอบไว้เป็นอย่างอื่น

ประกาศ ณ วันที่ ๑๗ ตุลาคม พ.ศ. ๒๕๖๕

(นายเทพสุ บวรโชติดารา)
รองเลขาธิการฯ รักษาราชการแทน
เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน



คู่มือการลงทะเบียนผู้ใช้งาน (User Registration)

เพื่อขอรับบริการงานระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ ของสำนักงานป้องกันและปราบปรามการฟอกเงิน

ศูนย์เทคโนโลยีสารสนเทศ

พฤศจิกายน ๒๕๖๖

สารบัญ

คู่มือการลงทะเบียนผู้ใช้งาน (User Registration)

เรื่อง ขอรับบริการงานระบบเทคโนโลยีสารสนเทศของสำนักงาน ปปง. **หมายเลขเอกสาร : ๐๑**

- แบบฟอร์มการขอสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ สำนักงาน ปปง. (แบบฟอร์ม สกท – ๐๐๑)

เรื่อง ขอรับบริการงานระบบเครือข่ายคอมพิวเตอร์ (LAN/Wi-Fi) ของสำนักงาน ปปง. **หมายเลขเอกสาร : ๐๒**

- แบบฟอร์มลงทะเบียนใช้งานระบบเครือข่ายของสำนักงาน ปปง. (LAN/Wi-Fi)

๑. วัตถุประสงค์ (Objective)

เพื่อเป็นคู่มือประกอบการปฏิบัติงานให้บริการ การขอสิทธิผู้ใช้งานใหม่/ขอปรับปรุงสิทธิ/ขอยกเลิกสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ สำนักงาน ปปง. (แบบฟอร์ม สกท – ๐๐๑) ให้มีมาตรฐานและถือปฏิบัติในแนวทางเดียวกัน

๒. ขอบเขต (Scope)

ครอบคลุมขั้นตอนการขอสิทธิผู้ใช้งานใหม่/ขอปรับปรุงสิทธิ/ขอยกเลิกสิทธิ การใช้งานระบบเทคโนโลยีสารสนเทศ สำนักงาน ปปง.

๓. คำจำกัดความ (Definition)

๓.๑ ผู้บังคับบัญชา หมายถึง ผู้อำนวยการกอง/ศูนย์/กลุ่ม และหัวหน้าศูนย์ ของผู้ขอใช้งาน/ผู้ขอใช้บริการ

๓.๒ ศท. หมายถึง ศูนย์เทคโนโลยีสารสนเทศ

๓.๓ ผอ.ศท. หมายถึง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๓.๔ ผอ.สกท. หมายถึง ผู้อำนวยการส่วนบริหารจัดการระบบเทคโนโลยีสารสนเทศ

๓.๕ เจ้าหน้าที่ส่วนบริหารจัดการระบบเทคโนโลยีสารสนเทศ (เจ้าหน้าที่ สกท.) หมายถึง ข้าราชการส่วนบริหารจัดการระบบเทคโนโลยีสารสนเทศที่ได้รับมอบหมาย ให้ทำหน้าที่ผู้ดูแลระบบเทคโนโลยีสารสนเทศ

๓.๖ ผู้ขอใช้งาน/ผู้ขอใช้บริการ หมายถึง เจ้าหน้าที่ผู้มีหน้าที่เกี่ยวข้อง ที่จำเป็นต้องใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน ปปง. ตามอำนาจหน้าที่และความรับผิดชอบ เช่น ข้าราชการ พนักงานราชการ ลูกจ้าง ของสำนักงาน ปปง. ที่ได้รับอนุญาตให้ใช้งานระบบฯ ของสำนักงาน ปปง. ได้

๔. หน้าที่ความรับผิดชอบ (Responsibility)

๔.๑ ผู้บังคับบัญชาของผู้ขอใช้งาน/ผู้ขอใช้บริการ มีหน้าที่พิจารณาลงนามอนุญาตในแบบฟอร์มการขอสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ สำนักงาน ปปง. (แบบฟอร์ม สกท – ๐๐๑)

๔.๒ ผอ.ศท. มีหน้าที่พิจารณาลงนามสั่งการส่วนบริหารจัดการระบบเทคโนโลยีสารสนเทศเพื่อดำเนินการกำหนดสิทธิผู้ใช้งานใหม่/ปรับปรุงสิทธิ/ยกเลิกสิทธิ ตามที่ระบุในแบบฟอร์ม สกท – ๐๐๑

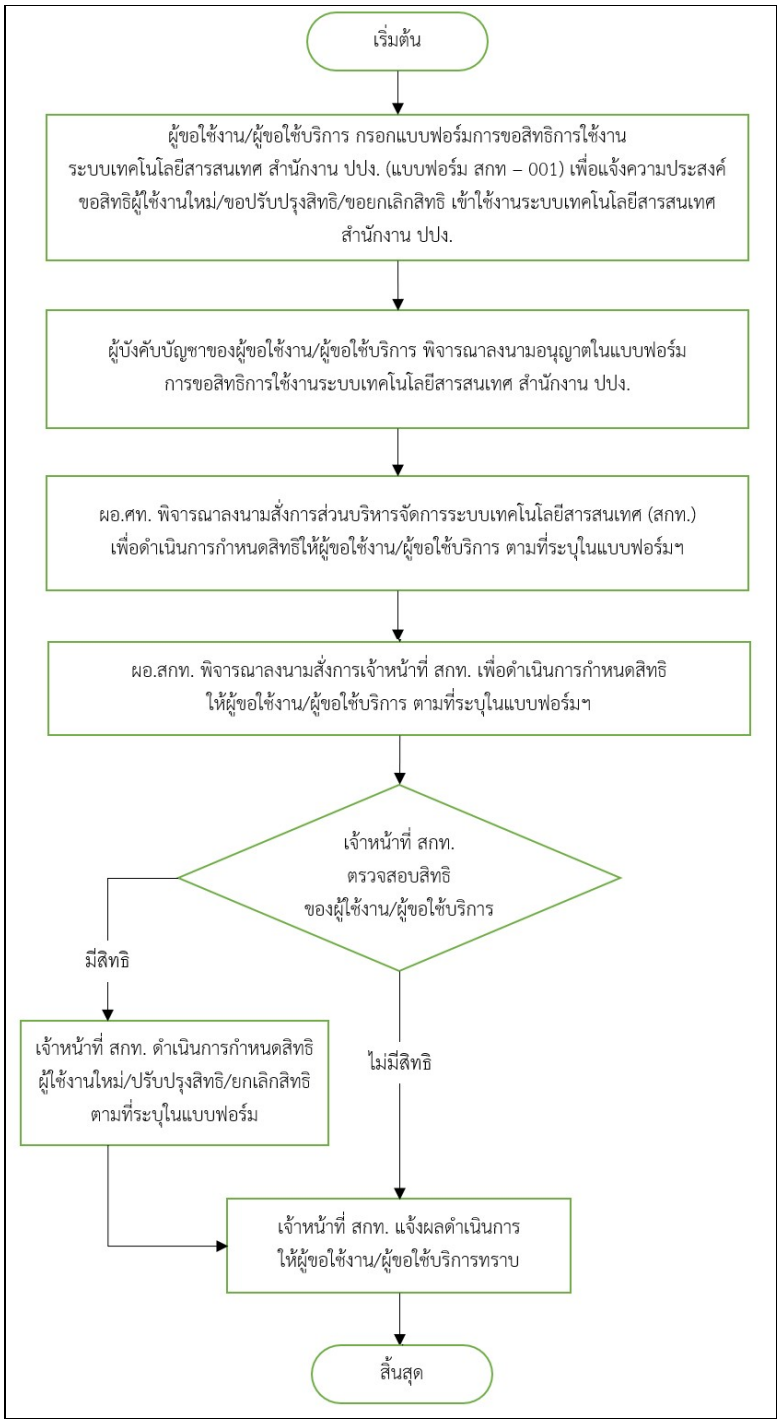
๔.๓ ผอ.สกท. มีหน้าที่พิจารณาลงนามสั่งการเจ้าหน้าที่ส่วนบริหารจัดการระบบเทคโนโลยีสารสนเทศเพื่อดำเนินการตรวจสอบก่อนกำหนดสิทธิผู้ใช้งานใหม่/ปรับปรุงสิทธิ/ยกเลิกสิทธิ ตามที่ระบุในแบบฟอร์ม สกท – ๐๐๑

๔.๔ เจ้าหน้าที่ส่วนบริหารจัดการระบบเทคโนโลยีสารสนเทศมีหน้าที่ตรวจสอบและกำหนดสิทธิผู้ใช้งานใหม่/ปรับปรุงสิทธิ/ยกเลิกสิทธิ ตามที่ระบุในแบบฟอร์ม สกท – ๐๐๑ และแจ้งผลให้ผู้ขอใช้งาน/ผู้ขอใช้บริการทราบ

๔.๕ ผู้ขอใช้งาน/ผู้ขอใช้บริการ ของสำนักงาน ปปง. มีหน้าที่กรอกข้อมูลแจ้งความประสงค์ในแบบฟอร์ม สกท – ๐๐๑ และตรวจสอบสิทธิที่ได้รับว่าสามารถเข้าถึง/เข้าใช้งานระบบเทคโนโลยีสารสนเทศตามที่ระบุในแบบฟอร์มฯ ได้อย่างครบถ้วน ถูกต้อง

๕. ขั้นตอนการปฏิบัติ (Procedure)

๕.๑ แผนผังการทำงาน



๕.๒ คำอธิบายขั้นตอน

๕.๒.๑ ผู้ขอใช้งาน/ผู้ขอใช้บริการ กรอกแบบฟอร์มการขอสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ สำนักงาน ปปง. (แบบฟอร์ม สกท – ๐๐๑) เพื่อแจ้งความประสงค์ขอสิทธิผู้ใช้งานใหม่/ขอปรับปรุงสิทธิ/ขอยกเลิกสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ สำนักงาน ปปง. (สามารถดาวน์โหลดแบบฟอร์มฯ ได้ด้วยตนเองผ่านทางเว็บไซต์สำนักงาน ปปง.)

๕.๒.๒ ผู้บังคับบัญชาของผู้ขอใช้งาน/ผู้ขอใช้บริการ พิจารณาลงนามอนุญาตในแบบฟอร์ม สกท – ๐๐๑ แล้วส่งแบบฟอร์มฯ ให้ ศท.

๕.๒.๓ ผอ.ศท. พิจารณาลงนามสั่งการส่วนบริหารจัดการระบบเทคโนโลยีสารสนเทศ เพื่อดำเนินการกำหนดสิทธิผู้ใช้งานใหม่/ปรับปรุงสิทธิ/ยกเลิกสิทธิ ตามที่ระบุในแบบฟอร์ม สกท – ๐๐๑

๕.๒.๔ ผอ.สกท. พิจารณาลงนามสั่งการเจ้าหน้าที่ส่วนบริหารจัดการระบบเทคโนโลยีสารสนเทศ เพื่อดำเนินการกำหนดสิทธิผู้ใช้งานใหม่/ปรับปรุงสิทธิ/ยกเลิกสิทธิ ตามที่ระบุในแบบฟอร์ม สกท – ๐๐๑

๕.๒.๕ เจ้าหน้าที่ สกท. ตรวจสอบสิทธิของผู้ใช้งาน/ผู้ขอใช้บริการ ตามตารางแสดงหน่วยงาน กอง/ศูนย์/กลุ่ม ที่มีสิทธิใช้งานระบบเทคโนโลยีสารสนเทศ สำนักงาน ปปง. ก่อนดำเนินการกำหนดสิทธิผู้ใช้งานใหม่/ปรับปรุงสิทธิ/ยกเลิกสิทธิ ตามที่ระบุในแบบฟอร์ม สกท – ๐๐๑

๕.๒.๖ เจ้าหน้าที่ สกท. แจ้งผลให้ผู้ขอใช้งาน/ผู้ขอใช้บริการทราบ เพื่อให้ตรวจสอบสิทธิที่ได้รับว่าสามารถเข้าถึง/เข้าใช้งานระบบเทคโนโลยีสารสนเทศ ตามที่ระบุในแบบฟอร์มฯ ได้อย่างครบถ้วน ถูกต้อง

๖. แบบฟอร์มที่ใช้ (Forms)

แบบฟอร์มการขอสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ สำนักงาน ปปง. (แบบฟอร์ม สกท – ๐๐๑)

ศูนย์เทคโนโลยีสารสนเทศ ส่วนบริหารจัดการระบบเทคโนโลยีสารสนเทศ

แบบฟอร์มการขอสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ สำนักงาน ปปง.

<u>ส่วนที่ ๑</u> ผู้ขอใช้บริการ วันที่ขอรับบริการ .....

ประเภทบุคลากร ☐ ข้าราชการ ☐ พนักงานราชการ ☐ ลูกจ้างประจำ ☐ ลูกจ้างชั่วคราว ☐ อื่นๆ ระบุ.....

คำนำหน้าชื่อ ..... เลขประจำตัวประชาชน ๑๓ หลัก .....

ชื่อ – นามสกุล (ไทย).....

ชื่อ – นามสกุล (อังกฤษ) .....

กอง / ศูนย์ / กลุ่ม ..... ส่วนงาน .....

ตำแหน่ง ..... เบอร์โทรศัพท์ภายใน ..... อีเมล .....

<u>ส่วนที่ ๒</u> รายละเอียดการขอใช้บริการระบบเทคโนโลยีสารสนเทศ สำนักงาน ปปง.

☐ ขอสิทธิผู้ใช้งานใหม่ ☐ ขอเพิ่มสิทธิ ☐ ขอยกเลิกสิทธิ

ระบบเทคโนโลยีสารสนเทศ สำนักงาน ปปง.	การใช้งาน
๑. ระบบการส่งรายงานธุรกรรมทางสื่ออิเล็กทรอนิกส์ (AERS)	
๒. ระบบสารสนเทศเพื่อรองรับการรายงานธุรกรรมฯ ตามมาตรา ๑๖ (ERS)	
๓. ระบบประสานข้อมูลรายงานการทำธุรกรรมฯ (AMFICS)	
๔. ระบบสารสนเทศหลักขององค์กร (Core Business)	
๕. ระบบบริหารจัดการทรัพย์สินของสำนักงาน ปปง. (AMCATs)	
๖. ระบบรายงานการทำธุรกรรมเงินสดผ่านแดนโดยใช้สื่ออิเล็กทรอนิกส์ (ECB)	
๗. ระบบสารสนเทศฐานข้อมูลสัมพันธ์ เพื่อตรวจสอบการกระทำความผิดมูลฐาน/ความผิดฟอกเงิน (AMCIS)	
๘. ระบบสารสนเทศเพื่อการประเมินความเสี่ยงและบริหารจัดการคดีของผู้มีหน้าที่รายงาน (AMRAC)	
๙. ระบบบริหารจัดการการประมูลทรัพย์สินที่ถูกยึดเพื่อการขายทอดตลาด (Auction)	
๑๐. ระบบบริหารจัดการการแบ่งปันข้อมูลสำหรับหน่วยงานภาครัฐ (Data Sharing)	
๑๑. ระบบรับเรื่องร้องเรียนแจ้งเบาะแส (Call Center ๑๗๑๐) และ ระบบตอบรับโทรศัพท์อัตโนมัติ (IVR Call Center)	
๑๒. ระบบเชื่อมโยงระบบบูรณาการฐานข้อมูลประชาชนและการบริการภาครัฐ (AMLINK)	
๑๓. ระบบตรวจสอบรายชื่อบุคคลที่มีความเสี่ยงสูงด้านการฟอกเงินและรายชื่อบุคคลที่ถูกกำหนด (APS)	
๑๔. ระบบศูนย์ข้อมูลคดีฟอกเงิน (ML Case Info)	
๑๕. ระบบบริหารจัดการฐานข้อมูลขนาดใหญ่ และซอฟต์แวร์ระบบวิเคราะห์ข้อมูลอัจฉริยะ (BI)	
๑๖. ระบบสนับสนุนและสั่งการปฏิบัติงานภาคสนาม (TOS)	
๑๗. ระบบอัตโนมัติเพื่อรวบรวมข่าวสาร (Web Crawler)	
๑๘. ระบบบริหารจัดการฝึกอบรมและการประเมินความรู้ในเรื่องกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน (ATS)	
๑๙. ระบบติดตามและบริหารจัดการบัญชีทรัพย์สินในคดี สำหรับสนับสนุนการบริหารกองทุนฯ (AFMS)	
๒๐. ระบบสนับสนุนการวิเคราะห์ธุรกรรมทางการเงิน (FTAS)	
๒๑. ระบบเว็บไซต์สำนักงาน ปปง. (www.amlo.go.th)	
๒๒. ระบบเอกสารข้อมูลทางอิเล็กทรอนิกส์ (AMDOC) และระบบสารสนเทศเพื่อบริหารจัดการภายในองค์กร (MIS)	
๒๓. ระบบสารสนเทศของการบริหารทั่วไปของสำนักงาน ปปง. (Back Office)	
๒๔. ระบบฐานข้อมูลสถิติและระบบติดตามประเมินผลเพื่อการบริหารจัดการ (KPIMS)	
๒๕. ระบบใบรับรองเงินเดือนและหนังสือรับรองการหักภาษี ณ ที่จ่าย ประจำปี (Pay Slip)	
๒๖. ระบบจดหมายอิเล็กทรอนิกส์ (e-mail)	
๒๗. ระบบจองห้องประชุมออนไลน์ (https://eservice.amlo.go.th)	

ระบบเทคโนโลยีสารสนเทศ สำนักงาน ปปง. (ต่อ)	การใช้งาน
๒๘. ระบบติดตามคดี (Case Tracking)	
๒๙. ระบบงานสารบรรณอิเล็กทรอนิกส์ (e-Saraban)	
๓๐. ระบบคุ้มครองสิทธิผู้เสียหาย (khumkrongsit)	
๓๑. ระบบสนับสนุนการรายงาน Work From Home	
๓๒. ระบบฐานข้อมูลสถิติด้าน AML/CFT	
๓๓. ระบบค้นหาข้อมูลบุคคลล้มละลาย (AMLO Bankrupt)	
๓๔. ระบบฐานข้อมูลการสำรวจทรัพย์สินประเภทอสังหาริมทรัพย์บนแผนที่อิเล็กทรอนิกส์เพื่อการบริหารจัดการทรัพย์สินที่ยึดหรืออายัด (e-Survey)	
๓๕. การลาออนไลน์ ผ่านระบบสารสนเทศทรัพยากรบุคคล (DPIS6)	

ใช้สัญลักษณ์ ✓ เพื่อเลือกระบบที่ต้องการขอใช้บริการ และใช้สัญลักษณ์ ✕ เพื่อขอยกเลิกการใช้งานระบบ

ข้าพเจ้าขอรับรองว่า ข้อมูลข้างต้นเป็นความจริง และรับทราบนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงาน ปปง. และจะปฏิบัติตามระเบียบและข้อกำหนด ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ทุกประการ

ลงชื่อผู้ขอใช้บริการ .....

(.....)

<u>ส่วนที่ ๓</u> ผู้บังคับบัญชาพิจารณา

เรียน ผอ.ศท.

พิจารณาแล้ว เห็นควรอนุญาต

(ผอ.กอง/ศูนย์/กลุ่ม) ลงชื่อ.....

(.....)

ตำแหน่ง .....

วันที่ .....

<u>ส่วนที่ ๔</u> ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศพิจารณา

เรียน ผอ.สกท.

ดำเนินการในส่วนที่เกี่ยวข้อง

ลงชื่อ.....

(.....)

ตำแหน่ง .....

วันที่ .....

<u>ส่วนที่ ๕</u> สำหรับเจ้าหน้าที่ส่วนบริหารจัดการระบบเทคโนโลยีสารสนเทศ

..... ดำเนินการในส่วนที่เกี่ยวข้อง

ลงชื่อ.....

(.....)

ตำแหน่ง .....

วันที่ .....

ลงชื่อ.....(ผู้ดำเนินการ)

(.....)

ตำแหน่ง .....

วันที่ .....

<u>ส่วนที่ ๖</u> สำหรับผู้ขอใช้บริการ

ได้รับสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน ปปง. ตามที่ขอใช้งานเรียบร้อยแล้ว

ลงชื่อ.....(ผู้ขอใช้บริการ)

(.....)

ตำแหน่ง .....

วันที่ .....

คำอธิบาย ระบบเทคโนโลยีสารสนเทศ

สิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ จำแนกตามหน่วยงาน

คู่มือการลงทะเบียนผู้ใช้งาน (User Registration)

แบบฟอร์มฯ ออก ณ วันที่ ๑๖ พฤศจิกายน ๒๕๖๖

๑. วัตถุประสงค์ (Objective)

เพื่อเป็นแนวทางในการขอรับบริการเข้าใช้งานระบบเครือข่ายภายในของสำนักงาน ปปง.

๒. ขอบเขต (Scope)

ครอบคลุมขั้นตอนการดำเนินการขอรับบริการเข้าใช้งานระบบเครือข่ายภายในของสำนักงาน ปปง.

๓. คำจำกัดความ (Definition)

๓.๑ ผอ.สคม. หมายถึง ผู้อำนวยการส่วนคอมพิวเตอร์และความมั่นคงปลอดภัยไซเบอร์

๓.๒ เจ้าหน้าที่ สคม. หมายถึง ข้าราชการส่วนคอมพิวเตอร์และความมั่นคงปลอดภัยไซเบอร์

๓.๓ ผู้ขอใช้งาน หมายถึง ผู้ขอใช้ระบบเครือข่ายของสำนักงาน ปปง. (LAN/Wi-Fi)

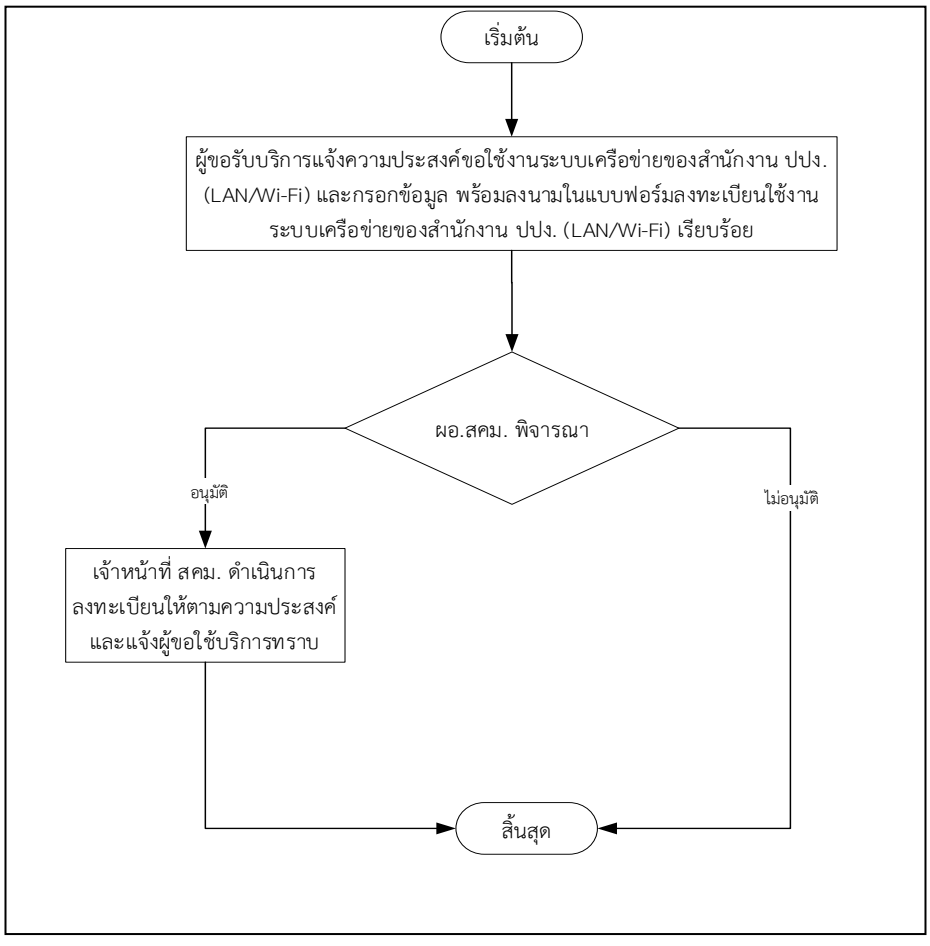
๔. หน้าที่ความรับผิดชอบ (Responsibility)

๔.๑ ผอ.สคม. มีหน้าที่อนุมัติ/ไม่อนุมัติในการขอรับบริการเข้าใช้งานระบบเครือข่ายภายในของสำนักงาน ปปง.

๔.๒ เจ้าหน้าที่ สคม. มีหน้าที่ดำเนินการตามคำขอรับบริการเข้าใช้งานระบบเครือข่ายภายในของสำนักงาน ปปง.

๕. ขั้นตอนการปฏิบัติ (Procedure)

๕.๑ แผนผังการทำงาน



๕.๒ คำอธิบายขั้นตอน

๕.๒.๑ ผู้ขอรับบริการแจ้งความประสงค์ขอรับบริการเข้าใช้งานระบบเครือข่ายภายในของสำนักงาน ปปง. ผอ.สคม. พิจารณาอนุมัติ/ไม่อนุมัติ

๕.๒.๒ กรณีอนุมัติเจ้าหน้าที่ สคม. ดำเนินการเพิ่มสิทธิ์เข้าใช้งานระบบเครือข่ายของสำนักงาน ปปง. ให้บุคคลนั้น ๆ และแจ้งให้ผู้ขอรับบริการทราบ

๕.๒.๓ กรณีไม่อนุมัติหรือเหตุอื่นใดถือเป็นอันยุติเรื่อง

๖. แบบฟอร์มที่ใช้ (Forms)

แบบฟอร์มลงทะเบียนขอรับบริการเข้าใช้งานระบบเครือข่ายภายในของสำนักงาน ปปง.

แบบฟอร์มลงทะเบียนเครื่องคอมพิวเตอร์ส่วนตัวหรืออุปกรณ์อิเล็กทรอนิกส์ (มือถือ แท็บเล็ต)

ใช้งานผ่านระบบเครือข่ายภายในของสำนักงาน ปปง.

หมายเลขอ้างอิง

ชื่อผู้ใช้งาน .....

สถานะผู้ใช้งาน ○ ข้าราชการ ○ พนักงานราชการ ○ ลูกจ้างชั่วคราว ○ อื่น ๆ.....

หน่วยงาน.....เบอร์โทรศัพท์.....

มีความประสงค์ขอใช้งานระบบเครือข่ายของสำนักงาน ปปง. ประเภท ○ LAN ○ Wi-Fi

ประเภทอุปกรณ์ ○ Notebook ○ Mobile ○ Tablet ○ PC

ยี่ห้อ.....

รุ่น.....

**MAC Address.....

ระบบปฏิบัติการ ○ Windows ○ Mac OS ○ Android ○ iOS ○ อื่น ๆ.....

วัตถุประสงค์ขอใช้งานเพื่อ ○ ปฏิบัติงาน ○ ติดต่อสื่อสาร ○ อื่น ๆ.....

.....

ผู้ขอใช้บริการ .....

( )

ตำแหน่ง.....

วันที่.....

สำหรับ ผู้บังคับบัญชาของผู้ขอใช้บริการ	สำหรับ เจ้าหน้าที่ผู้ปฏิบัติ
○ อนุญาต ○ ไม่อนุญาต เหตุผล..... ..... ลงชื่อ..... ( ) ตำแหน่ง ..... วันที่.....	○ ดำเนินการเรียบร้อย ○ ไม่สามารถดำเนินการได้ เหตุผล .... ลงชื่อ..... ( ) ตำแหน่ง ..... วันที่.....