ประกาศสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) พ.ศ. ๒๕๖๕

อาศัยตามความในมาตรา ๕ มาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของสถาบันวิจัยและพัฒนาพื้นที่สูง เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ สถาบันวิจัยและพัฒนาพื้นที่สูง จึงได้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ ตามประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) พ.ศ. ๒๕๖๕”

ข้อ ๒ วัตถุประสงค์

๒.๑ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๒ เพื่อให้เกิดความเชื่อมั่นและความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) ให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๓ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) ได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

ข้อ ๓ ขอบเขตการดำเนินงาน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) มีขอบเขตครอบคลุม ดังนี้

ส่วนที่ ๑ นโยบายการควบคุมการเข้าถึงและการใช้งานสารสนเทศ มีสาระสำคัญประกอบด้วย

/๑.๑ การเข้าถึง...

๑.๑ การเข้าถึงและควบคุมการใช้งานสารสนเทศ
๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน
๑.๓ การควบคุมการเข้าถึงห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย
๑.๔ การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
๑.๕ การควบคุมการเข้าถึงระบบเครือข่าย
๑.๖ การควบคุมการเข้าถึงระบบปฏิบัติการ
๑.๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
๑.๘ การควบคุมการใช้งานอินเทอร์เน็ต
๑.๙ การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์
๑.๑๐ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
๑.๑๑ การใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์
๑.๑๒ การสร้างความมั่นคงปลอดภัยด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ ๒ นโยบายการจัดทำระบบสำรองของระบบสารสนเทศและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

ส่วนที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๔ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๔ การกำหนดความรับผิดชอบ

๔.๑ ระดับนโยบาย

กำหนดให้ผู้อำนวยการสถาบันวิจัยและพัฒนาพื้นที่สูง เป็นผู้รับผิดชอบ ต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้ใดผู้หนึ่ง อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กำหนดให้ผู้อำนวยการสำนักยุทธศาสตร์และแผน เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) รวมถึงเป็นผู้ติดตาม กำกับดูแล ควบคุม ตรวจสอบ ให้ข้อเสนอแนะและคำปรึกษาแก่เจ้าหน้าที่ในการปฏิบัติงาน

๔.๒ ระดับปฏิบัติ

๔.๒.๑ นโยบายการควบคุมการเข้าถึงและการใช้งานสารสนเทศ ผู้รับผิดชอบ ได้แก่
๔.๒.๑.๑ ศูนย์ข้อมูลและสารสนเทศ
๔.๒.๑.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย
๔.๒.๑.๓ เจ้าหน้าที่ที่ได้รับมอบหมาย
๔.๒.๑.๔ ผู้ใช้งาน

๔.๒.๒ นโยบายการจัดทำระบบสำรองของระบบสารสนเทศ ผู้รับผิดชอบ ได้แก่
๔.๒.๒.๑ ศูนย์ข้อมูลและสารสนเทศ
๔.๒.๒.๒ ผู้ดูแลระบบที่ได้รับมอบหมาย
๔.๒.๒.๓ เจ้าหน้าที่ที่ได้รับมอบหมาย

/๔.๒.๓ นโยบาย....

๔.๒.๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

๔.๒.๓.๑ ศูนย์ข้อมูลและสารสนเทศ

๔.๒.๓.๒ ผู้ตรวจสอบภายใน หรือ ผู้ตรวจสอบจากภายนอก

๔.๒.๓.๓ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒.๔ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้รับผิดชอบ ได้แก่

๔.๒.๔.๑ ศูนย์ข้อมูลและสารสนเทศ

๔.๒.๔.๒ หน่วยงานที่ได้รับมอบหมายในการฝึกอบรม

๔.๒.๔.๓ ผู้ดูแลระบบที่ได้รับมอบหมาย

๔.๒.๔.๔ เจ้าหน้าที่ที่ได้รับมอบหมาย

ข้อ ๕ ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมถึงทบทวนปรับปรุงนโยบายและแนวปฏิบัติอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๖ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ เรื่อง “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) พ.ศ. ๒๕๖๕” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) และหน่วยงานภายนอก ต้องถือปฏิบัติตามอย่างเคร่งครัด

โดยให้ยกเลิกประกาศนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) พ.ศ. ๒๕๕๘ ลงวันที่ ๑๑ สิงหาคม พ.ศ. ๒๕๕๘ และให้ใช้ประกาศฉบับนี้แทน

ทั้งนี้ ตั้งแต่วันที่ 9 เมษายน พ.ศ. ๒๕๖๕ เป็นต้นไป

(นางสาวหินรัตน์ พิทักษ์พงศ์เจริญ)
รองผู้อำนวยการสถาบันวิจัยและพัฒนาพื้นที่สูง ด้านบริหารจัดการ
รักษาการแทนผู้อำนวยการสถาบันวิจัยและพัฒนาพื้นที่สูง

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สถาบันวิจัยและพัฒนาพื้นที่สูง
(องค์การมหาชน)

ปีงบประมาณ 2565

Highland
Research
and
Development
Institute
(Public Organization)

เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน)

หรือ สวพส.

ประจำปีงบประมาณ ๒๕๖๕

คำนำ

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลายมากขึ้นใน การให้ได้มาซึ่งข้อมูล สารสนเทศที่เป็นประโยชน์ต่อการดำเนินชีวิตของประชาชน การบริหารและการตัดสินใจใน การดำเนินภารกิจภาครัฐและธุรกิจภาคเอกชนรวมถึงการนำสารสนเทศมาใช้ในการกำหนดนโยบาย และการ พัฒนาประเทศ ขณะเดียวกันปัญหาความไม่น่าเชื่อถือของสารสนเทศอันเนื่องมาจากความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ โดยหัวใจสำคัญของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วย หลักแนวคิด CIA ประกอบด้วย Confidentiality (ความลับ) โดยข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ข้อมูลและระบบสารสนเทศจึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัยที่เพียงพอ ในการรักษาความลับของข้อมูลนั้น Integrity (ความถูกต้อง ความสมบูรณ์) รวมถึงความถูกต้องครบถ้วนของข้อมูล Availability (ความพร้อมใช้) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

ปัจจุบันพบปัญหาความมมั่นคงปลอดภัยในระบบสารสนนเทศ ที่มีรูปแบบหลากหลายส่งผลทวีความรุนแรงเพิ่มขึ้นทั้งในและต่างประเทศ ซึ่งเกิดปัญหาเนื่องมาจากช่องโหว่ หรือจุดอ่อนของระบบสารสนเทศ การขาดนโยบาย และแนวปฏิบัติ ด้านความมั่นคงปลอดภัยที่ชัดเจน และการนำมาตรการไปปฏิบัติอย่างมีประสิทธิภาพ

โดยคณะอนุกรรมการความมั่นคงปลอดภัยภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ขึ้น เพื่อเป็นแนวทางให้หน่วยงานของภาครัฐได้ใช้จัดทำแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ เพื่อช่วยให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานภาครัฐ มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือมากยิ่งขึ้น

สถาบันวิจัยและพัฒนาพื้นที่สูง จึงได้จัดทำนโยบายและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสถาบันวิจัยและพัฒนาพื้นที่สูง ประจำปีงบประมาณ ๒๕๖๕ ขึ้น เพื่อเผยแพร่ให้ทุกหน่วยงานในสถาบันวิจัยและพัฒนาพื้นที่สูง เพื่อให้บุคลากรทุกคนในสถาบันวิจัยและพัฒนาพื้นที่สูง มีความรู้ เข้าใจในนโยบายและแนวทาง ปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสถาบันวิจัยและพัฒนาพื้นที่สูง และสามารถนำไปประยุกต์ใช้ได้อย่างมีประสิทธิภาพ บรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยในระบบสารสนเทศของสถาบัน

สถาบันวิจัยและพัฒนาพื้นที่สูง

สารบัญ

๑. บทนำ

๑.๑ หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) หรือ สวพส. ได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้นเพื่อให้ระบบเทคโนโลยีสารสนเทศของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) มีการใช้งานอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัย ให้สามารถดำเนินงานได้อย่างต่อเนื่อง และป้องกันภัยคุกคามต่างๆ มีความปลอดภัยของข้อมูลสารสนเทศ และความเป็นมาตรฐานของการให้บริการข้อมูลสารสนเทศ อีกทั้งยังเป็นการลดโอกาสความเสี่ยงของข้อมูลสารสนเทศรวมถึงการป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ

๑.๒. วัตถุประสงค์

สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) ได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผลและปฏิบัติตามกฎหมายต่าง ๆ ที่เกี่ยวข้องได้อย่างถูกต้อง

๒.๒ เพื่อสร้างความตระหนักและส่งเสริมให้บุคลากร และบุคคลที่เกี่ยวข้องเกิดความรู้ ความเข้าใจ และให้ความสำคัญเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๒.๓ เพื่อป้องกันไม่ให้มีผู้กระทำหรือใช้วิธีการใดๆ ในการล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ

๒.๔ เพื่อรักษาความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอของระบบสารสนเทศ

๑.๓. องค์ประกอบของนโยบาย

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) ได้กำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงด้านสารสนเทศ โดยแบ่งแนวปฏิบัติออกเป็นส่วนๆ ดังต่อไปนี้

ส่วนที่ ๑ นโยบายการควบคุมการเข้าถึงและการใช้งานสารสนเทศ

๑. การเข้าถึงและควบคุมการใช้งานสารสนเทศ

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน

๓. การควบคุมการเข้าถึงห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย
๔. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
๕. การควบคุมการเข้าถึงระบบเครือข่าย
๖. การควบคุมการเข้าถึงระบบปฏิบัติการ
๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
๘. การควบคุมการใช้งานอิเล็กทรอนิกส์
๙. การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์
๑๐. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
๑๑. การใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์
๑๒. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ ๒ นโยบายการจัดทาระบบสำรองของระบบสารสนเทศและการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

ส่วนที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๔ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๔ บทบังคับใช้

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ให้มีผลบังคับใช้ครอบคลุมข้อมูลและระบบสารสนเทศของ สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) บุคลากรที่เกี่ยวข้องมีหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ภายใต้การสนับสนุน และติดตามการประยุกต์ใช้ โดยผู้อำนวยการสถาบันวิจัยและพัฒนาพื้นที่สูง

กรณีข้อมูลหรือระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูง (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๑.๕. การเผยแพร่และทบทวน

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) ฉบับนี้ จัดทำขึ้นและมีการทบทวนอย่างน้อยปีละ 1 ครั้ง โดยนโยบายและแนวปฏิบัติได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบภายในสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) เพื่อให้บุคลากรของสถาบันวิจัยและพัฒนาพื้นที่สูง และบุคคลภายนอกที่เกี่ยวข้องได้ทราบและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒. คำนิยาม

คำนิยามที่ใช้ในแนวนโยบายและแนวปฏิบัตินี้ ประกอบด้วย

คำนิยาม	ความหมาย หรือ คำจำกัดความ
๑. หน่วยงาน หรือ องค์กร	สถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) หรือ สวพส.
๒. หัวหน้างาน	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) หรือ สวพส.
๓. ผู้ใช้งาน หรือ ผู้ใช้บริการ	เจ้าหน้าที่ พนักงาน ลูกจ้างตามสัญญาจ้างในสังกัด สวพส. และหมายรวมถึงบุคคลที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของ สวพส.
๔. ผู้ดูแลระบบ (System Administrator)	ผู้ที่ได้รับมอบหมายจากผู้อำนวยการให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบเครือข่ายและคอมพิวเตอร์ไม่ว่าส่วนหนึ่งส่วนใด
๕. ผู้ตรวจสอบภายในหน่วยงานของรัฐ	ผู้ให้บริการแก่ผู้บริหาร การให้ความเชื่อมั่นและการให้คำปรึกษาอย่างเที่ยงธรรมและเป็นอิสระ เพื่อเพิ่มคุณค่าและปรับปรุงการดำเนินงานของ สวพส. ให้ดีขึ้นให้บรรลุเป้าหมายและวัตถุประสงค์ที่กำหนดด้วยการประเมินและการปรับปรุงประสิทธิภาพ การประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุมภายในและความคุ้มค่าของการใช้เงิน รวมทั้งความถูกต้องเชื่อถือได้ของข้อมูลทางการเงิน ตลอดจนการปฏิบัติตามกฎระเบียบที่เกี่ยวข้อง
๖. หน่วยงานภายนอก	องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
๗. สิทธิ์ของผู้ใช้งาน	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
๘. ระบบคอมพิวเตอร์	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
๙. ระบบเครือข่าย	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น
๑๐. ระบบแลน (Local Area Network) และ ระบบอินทราเน็ต (Intranet)	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายใน สวพส. เข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายใน สวพส.

คำนิยาม	ความหมาย หรือ คำจำกัดความ
๑๑. ระบบอินเทอร์เน็ต (Internet)	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของ สวพส. เข้ากับเครือข่ายอินเทอร์เน็ตสากล
๑๒. ระบบเทคโนโลยีสารสนเทศ (Information Technology System)	ระบบงานของ สวพส. ที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่นำมาใช้ประโยชน์ในการวางแผนการบริหารการปฏิบัติงาน สนับสนุนการให้บริการ และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น
๑๓. เครื่องคอมพิวเตอร์ (Computer)	เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (Personal Computer) เครื่องคอมพิวเตอร์แบบพกพา (Notebook Computer) และเครื่องคอมพิวเตอร์แบบพกพา (Tablet Computer)
๑๔. ข้อมูลคอมพิวเตอร์ (Data)	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
๑๕. สารสนเทศ (Information)	ข้อเท็จจริงที่ได้จากการนำข้อมูลผ่านการประมวลผล จัดระเบียบข้อมูลอาจอยู่ในรูปของตัวเลข ข้อความ หรือ ภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผน การตัดสินใจ และอื่นๆ
๑๖. พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร	พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น
๑๖.๑. พื้นที่ทำงาน	พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูและระบบ (System Administrator)
๑๖.๒. พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย	พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์
๑๖.๓. พื้นที่ใช้งานระบบเครือข่ายไร้สาย	พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย
๑๗. สินทรัพย์ หรือ ทรัพย์สิน	ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ หมายรวมถึงสิ่งใดก็ตามที่มีคุณค่าสาหรับองค์กร
๑๘. จดหมายอิเล็กทรอนิกส์ (E-Mail)	ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

คำนิยาม	ความหมาย หรือ คำจำกัดความ
๑๙. บัญชีผู้ใช้บริการ (Account)	รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของ สวพส.
๒๐. ชื่อผู้ใช้ (Username)	ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้
๒๑. ลงบันทึกเข้า (Login)	กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้ระบบคอมพิวเตอร์และระบบเครือข่าย ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง
๒๒. ลงบันทึกออก (Logout)	กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย
๒๓. รหัสผ่าน (Password)	ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ
๒๔. โปรแกรมประสงค์ร้าย (Malware)	โปรแกรมคอมพิวเตอร์ชุดคำสั่งและ/หรือ ข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าทางตรงหรือทางอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) สปายแวร์ (Spyware) หนอน (Worm) ม้าโทรจัน (Torjan horse) ฟิชชิง (Phishing) จดหมายลูกโซ่ (Mass Mailing) เป็นต้น
๒๕. การตั้งค่าระบบ (Configuration)	ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์
๒๖. เลขที่อยู่ไอพี (IP Address)	ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)
๒๗. แบนด์วิดท์ (Bandwidth)	ปริมาณข้อมูลที่ ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล
๒๘. ช่องโหว่ (Vulnerability)	ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
๒๙. การเข้ารหัส (Encryption)	การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
๓๐. SSID (Service Set Identifier)	บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

คำนิยาม	ความหมาย หรือ คำจำกัดความ
๓๑. WPA (Wi-Fi Protected Access)	ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มี ความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)
๓๒. Wireless LAN Client	เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลน โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ โดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ ซึ่งมีมาตรฐานที่นิยมใช้เรียกว่า IEEE ๘๐๒.๑๑
๓๓. MAC Address (Media Access Control Address)	หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขที่จะมากับอีเทอร์เนตการ์ดโดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง
๓๔. VPN (Virtual Private Network)	เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
๓๕. Web Server	เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บและมีหน้าที่ให้บริการเว็บเพจต่างๆ
๓๖. ชื่อโดเมนย่อย (Sub Domain Name)	ส่วนย่อยที่จะช่วยขยายให้ทราบถึงกลุ่ม ต่าง ๆ ภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ “ที่อยู่เว็บไซต์” แทนได้
๓๗. อุปกรณ์กระจายสัญญาณข้อมูล (Switch)	อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ – ส่งข้อมูล
๓๘. อุปกรณ์จัดเส้นทาง (Router)	อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น
๓๙. อุปกรณ์กระจายสัญญาณ (Access Point)	อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย
๔๐. การพิสูจน์ยืนยันตัวตน (Authentication)	ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)
๔๑. แผนผังระบบเครือข่าย (Network Diagram)	แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน
๔๒. ไฟร์วอลล์ (Firewall)	เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย
๔๓. Firewall Log	การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟล์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถ

คำนิยาม	ความหมาย หรือ คำจำกัดความ
	นำมาใช้ในการวิเคราะห์ เพื่อตรวจสอบประเภทของการสื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน
๔๔. ข้อมูลจราจรทางคอมพิวเตอร์ (Log)	ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลาและชนิดของบริการอื่น ๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์
๔๕. การเข้าถึง หรือควบคุมการใช้งานสารสนเทศ	การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตบุคคลภายนอก
๔๖. ความมั่นคงปลอดภัย และความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)	ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน รวมถึงการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และ สภาพพร้อมใช้งาน (Availability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)
๔๗. เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)	กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
๔๘. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
๔๙. การสำรอง (Backup)	มีความหมายสองอย่าง คือ ☐ การสำรองเครื่องหรืออุปกรณ์คอมพิวเตอร์ เมื่อคอมพิวเตอร์หลักหรืออุปกรณ์ในคอมพิวเตอร์หลักเสีย จะสามารถนำมาใช้งานได้ทันที ☐ การสำรองข้อมูล ซึ่งในทางคอมพิวเตอร์หมายความถึง การเก็บสำรองข้อมูลที่อยู่ในสภาพก่อนที่จะเกิดการเสียหายไว้

คำนิยาม	ความหมาย หรือ คำจำกัดความ
๕๐. การกู้ข้อมูล (Recovery)	การนำข้อมูลที่เก็บสำรองไว้มาใช้แทนส่วนที่เสียหายหรือสูญหายไป หรือการกู้ระบบประมวลข้อมูลคอมพิวเตอร์ให้กลับมาอยู่ในสภาพก่อนที่ระบบจะเกิดความผิดพลาดหรือความล้มเหลว ความล้มเหลวของอุปกรณ์คอมพิวเตอร์หรือโปรแกรมที่ใช้งานก่อให้เกิดความเสียหายขึ้นทั้งสิ้น ไม่ว่าจะเป็นความเสียหายต่อระบบปฏิบัติการ (Operating System) หรือว่าระบบฐานข้อมูล (Database System) ทั้งนี้ การกู้ข้อมูลจะช่วยให้คอมพิวเตอร์กลับมาอยู่ในสภาพเดิมได้ การที่เกิดจุดผิดพลาดในระบบฐานข้อมูล ถ้าหากมีการตรวจเช็คพบควรที่จะทำการกู้ข้อมูลในทันที
๕๑. การพิสูจน์และยืนยันตัวตน	กระบวนการพิสูจน์และยืนยันความถูกต้องของตัวบุคคล
๕๒. ระบบการพิสูจน์และยืนยันตัวตนดิจิทัล	เครือข่ายทางอิเล็กทรอนิกส์ที่เชื่อมโยงข้อมูลระหว่างบุคคลใดๆ หรือหน่วยงานของรัฐเพื่อประโยชน์ในการพิสูจน์และยืนยันตัวตน และการทำธุรกรรมอื่นๆ ที่เกี่ยวเนื่องกับการพิสูจน์และยืนยันตัวตน
๕๓. ระบบแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์อัตโนมัติ	โปรแกรมคอมพิวเตอร์ หรือวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอัตโนมัติอื่น ที่ใช้เพื่อที่จะทำให้เกิดการกระทำหรือการตอบสนองต่อข้อมูลอิเล็กทรอนิกส์หรือการปฏิบัติการใด ๆ ต่อระบบข้อมูล ไม่ว่าทั้งหมดหรือแต่บางส่วน โดยปราศจากการตรวจสอบหรือการแทรกแซงโดยบุคคลธรรมดาในแต่ละครั้งที่มีการดำเนินการหรือแต่ละครั้งที่ระบบได้สร้างการตอบสนอง

ส่วนที่ ๑
นโยบายการควบคุมการเข้าถึงและการใช้งานสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานสารสนเทศของ สวพส. ป้องกันการบุกรุกผ่านระบบเครือข่ายหรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่าย รวมทั้งสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานสนเทศขององค์กรได้อย่างถูกต้อง

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้องได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์แลพแผน
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย
๔. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Information Access Control)

เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลให้มีความมั่นคงปลอดภัย ให้ปฏิบัติอย่างน้อยดังนี้

๑.๑ จัดทำบัญชีสินทรัพย์ ซึ่งจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยกำหนดกลุ่มผู้ใช้งานและสิทธิผู้ใช้งาน

๑.๒ กำหนดเกณฑ์ในการขออนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการขออนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

๑.๒.๑ กำหนดสิทธิของกลุ่มผู้ใช้งาน แบ่งออกเป็น
๑.๒.๑.๑ สิทธิอ่านอย่างเดียว
๑.๒.๑.๒ สิทธิสร้างข้อมูล
๑.๒.๑.๓ สิทธิป้อนข้อมูล
๑.๒.๑.๔ สิทธิแก้ไข
๑.๒.๑.๕ สิทธิอนุมัติ
๑.๒.๑.๖ ไม่มีสิทธิ

๑.๒.๒ กำหนดเกณฑ์การระงับสิทธิ การมอบอำนาจ ให้เป็นไปตามที่กำหนดไว้ในการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่กำหนดไว้

๑.๓ ข้อกำหนดเกี่ยวกับประเภทข้อมูลหรือรูปแบบของเอกสารเล็กทรอนิกส์ แบ่งได้ดังนี้

๑.๓.๑ รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ เมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์และสามารถอ่านข้อความได้ ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ เช่น

๑.๓.๑.๑ Text Format

๑.๓.๑.๒ Document Form

๑.๓.๑.๓ PDF Form (Portable Document Format)

๑.๓.๑.๔ XML (Extensible Markup Language)

๑.๓.๒ รูปแบบเอกสารภาพ (Image) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ เช่น

๑.๓.๒.๑ JPEG or JPG Format

๑.๓.๒.๒ PNG or GIF Form

๑.๓.๒.๓ Bitmap Format

๑.๓.๓. ฐานข้อมูล (Database) หมายถึง ชุดของข้อมูลที่รวมเอาข้อมูลที่เกี่ยวข้องกันเป็นเรื่องราวเดียวกัน รวมกันเป็นกลุ่มหรือชุดข้อมูล เช่น ฐานข้อมูลผลการวิจัย ฐานข้อมูลผัก-ไม้ผลบนที่สูง ฐานข้อมูลข้อมูลด้านแผนที่ และฐานข้อมูลการใช้ประโยชน์ที่ดินรายแปลง เป็นต้น ซึ่งข้อมูลเหล่านี้ได้มาจากการบันทึกข้อมูลโดยผู้ใช้หรือบางข้อมูลอาจจะได้มาจากการประมวลผลข้อมูล และบันทึกข้อมูลกลับไปยังตำแหน่งที่ต้องการ

๑.๔ ลำดับชั้นความสำคัญหรือลำดับชั้นความลับของข้อมูล

ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์และรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยกำหนดกระบวนการและวิธีการต่อเอกสารที่สำคัญไว้ดังนี้

๑.๔.๑ การจัดแบ่งระดับความสำคัญของข้อมูล แบ่งออกเป็น

๑.๔.๑.๑ ข้อมูลลับมากที่สุด หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๑.๔.๑.๒ ข้อมูลลับมาก หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรง

๑.๔.๑.๓ ข้อมูลลับ หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหาย

๑.๔.๑.๔ ข้อมูลทั่วไป หมายถึง ข้อมูลที่ไม่มีความลับสามารถเปิดเผยได้

โดยกำหนดความรับผิดชอบให้แก่เจ้าของข้อมูลเป็นผู้พิจารณากำหนดระดับชั้นความลับของข้อมูล และการยกเลิกหรือปรับระดับชั้นความลับของข้อมูลตามความจำเป็น

๑.๔.๒ การรับส่งข้อมูลสำคัญระดับชั้นความลับ ตั้งแต่ชั้น “ลับ” ขึ้นไปผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล อ้างอิงตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔

๑.๕ การแบ่งระดับชั้นการเข้าถึงข้อมูล แบ่งออกเป็น

๑.๕.๑ เข้าถึงได้เฉพาะผู้ที่มีสิทธิสูงสุดในการบริหารจัดการระบบสารสนเทศ

๑.๕.๒ เข้าถึงได้เฉพาะผู้ที่ใช้ที่ได้รับอนุมัติสิทธิจากเจ้าของระบบงานแล้วเท่านั้น

๑.๕.๓ เข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง

๑.๕.๔ เข้าถึงได้ทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว

๑.๖ กำหนดเวลาที่เข้าถึงได้

๑.๖.๑ ในเวลาราชการ ได้แก่ วันจันทร์ - ศุกร์ เวลา ๐๘.๓๐ – ๑๖.๓๐ น.

๑.๖.๒. นอกเวลาราชการที่ได้รับอนุญาต ได้แก่ วันจันทร์–ศุกร์ เวลา ๑๖.๓๐–๑๙.๓๐ น.

๑.๖.๓. วันหยุดราชการและวันหยุดนักขัตฤกษ์ที่ได้รับอนุญาต ได้แก่ ๐๘.๓๐–๑๖.๓๐ น.

๑.๖.๔ เวลาอื่นตามที่ระบุไว้ให้เข้าถึงได้

๑.๗ การกำหนดช่องทางที่สามารถเข้าถึงได้ แบ่งออกเป็น

๑.๗.๑ อินทราเน็ต (Intranet)

๑.๗.๒ อินเทอร์เน็ต (Internet)

๑.๗.๓ จดหมายอิเล็กทรอนิกส์ (E-mail)

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาตให้ปฏิบัติอย่างน้อยดังนี้

๒.๑ การสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดมาตรการเชิงป้องกัน ดังนี้

๒.๑.๑ มีการเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้ใช้งานได้รับทราบ (Information Security Awareness)

๒.๑.๑ มีการฝึกอบรมหลักสูตรเพื่อสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) ให้ทราบถึงภัยและผลกระทบจากการใช้เทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงมาตรการเชิงป้องกันตามความเหมาะสม โดยจัดให้มีการอบรมผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

๒.๒ การกำหนดสิทธิ์ผู้ใช้งานให้สามารถใช้งานระบบต่างๆ

๒.๒.๑ การกำหนดสิทธิ์สำหรับผู้ใช้งานโดยตำแหน่ง

กลุ่มระบบเครือข่ายและคอมพิวเตอร์ ศูนย์ข้อมูลและสารสนเทศจะทำการกำหนดสิทธิ์การใช้ให้ผู้บริหารระดับสูง ผู้อำนวยการ/ สำนัก/ ศูนย์ฯ/ ผู้อำนวยการสำนัก/ กลุ่มงาน ของ สวพส. โดยกำหนดสิทธิ์ให้เข้าใช้งานระบบต่างๆ ดังนี้

๒.๒.๑.๑ ระบบ Internet

๒.๒.๑.๒ ระบบ Intranet

๒.๒.๑.๓ ระบบจดหมายอิเล็กทรอนิกส์

๒.๒.๑.๔ ระบบ MIS

๒.๒.๑.๕ ระบบสารสนเทศต่างๆ ขององค์กร เช่น

๑) ระบบประชุมทางไกล

๒) ระบบติดตามและประเมินผล

๒.๒.๒ การกำหนดสิทธิสำหรับผู้ใช้ส่วนบุคคล (Personal Account)

เจ้าหน้าที่ที่สามารถขอใช้งานระบบเครือข่ายของ สวพส. คือ ลูกจ้างประจำ เจ้าหน้าที่โครงการ และลูกจ้างชั่วคราว (จ้างเหมา) ของ สวพส. เท่านั้น โดยกำหนดสิทธิ์ให้เข้าใช้งานระบบต่างๆ ดังนี้

๒.๒.๒.๑ ระบบ Internet

๒.๒.๒.๒ ระบบ Intranet

๒.๒.๒.๓ ระบบจดหมายอิเล็กทรอนิกส์

๒.๒.๒.๔ ระบบ MIS

๒.๓ การลงทะเบียนผู้ใช้งาน (User Registration)

การลงทะเบียนผู้ใช้งาน (User Registration) มีขั้นตอนการปฏิบัติ คือ กำหนดให้ลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาต โดยมีรายละเอียดดังนี้

๒.๓.๑ ขั้นตอนการขอลงทะเบียนสมัครใช้งานระบบเครือข่าย สวพส.

๒.๓.๑.๑ ผู้สมัครกรอกข้อมูลลงในแบบฟอร์ม โดยขอรับแบบฟอร์มได้ที่กลุ่มงานบริหารทรัพยากรมนุษย์หรือศูนย์ข้อมูลและสารสนเทศ

๒.๓.๑.๒ กลุ่มงานบริหารทรัพยากรมนุษย์ทำการแจ้งชื่อผู้ใช้และรหัสผ่านให้กับผู้สมัคร

*หมายเหตุ ผู้สมัครต้องเป็นเจ้าหน้าที่หรือพนักงานใน สวพส. เท่านั้น

๒.๓.๒ ขั้นตอนการเปลี่ยนแปลงรหัสผ่านจากสมาชิกระบบเครือข่าย สวพส.

๒.๓.๒.๑ สมาชิกระบบเครือข่ายที่มีความประสงค์จะปลี่ยนแปลงรหัสผ่าน (Password) ให้เข้าไปที่ URL ของ สวพส. คือ changepass.hrdi.or.th

๒.๔ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

แนวทางการบริหารจัดการสิทธิของผู้ใช้งาน (ส่วนของผู้ดูแลระบบ)

๒.๔.๑ เมื่อได้รับแบบฟอร์มขอใช้ระบบเครือข่าย ผู้ดูแลระบบจะทำการตรวจสอบชื่อผู้สมัครจากบัญชีผู้ใช้งานระบบเครือข่ายของ สวพส. ว่าเป็นสมาชิกอยู่หรือไม่

๒.๔.๒ ตรวจสอบรายชื่อผู้สมัครกรณีที่เป็นสมาชิกอยู่แล้ว จะติดต่อแจ้งการมีสิทธิกับผู้สมัครโดยตรง

๒.๔.๓ กรณีที่ยังไม่เคยเป็นสมาชิก จะทำการกำหนดสิทธิการใช้งานระบบและทำบันทึกโดย เจ้าหน้าที่ศูนย์ข้อมูลและสารสนเทศ

๒.๔.๔ ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

๒.๔.๕ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

๒.๔.๕.๑ ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงาน

๒.๔.๕.๒ ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๒.๔.๕.๓ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีที่พ้นกำหนดการให้สิทธิพิเศษ

๒.๔.๖. การกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบ Internet และ ระบบ Intranet เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบ รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๕ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

การบริหารจัดการรหัสผ่านสาหรับผู้ใช้งาน สวพส. แบ่งเป็น ๒ วิธี ดังนี้

วิธีที่ ๑ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน โดยผู้ดูแลระบบ (Admin) เป็นผู้บันทึก/แก้ไข/ลบข้อมูล ข้อมูลรหัสผู้ใช้งานจำแนกเป็น ๒ ประเภทย่อย คือ

๒.๕.๑ ประเภทที่ ๑ เป็นระบบที่มีความเสี่ยงสูงและมีมาตรการป้องกัน เช่น ระบบ Authentication ระบบ Proxy ระบบ Firewall ระบบ IPS และระบบควบคุมการเข้าถึงระบบ/ข้อมูล (Access Control) ระบบเครือข่ายไร้สาย (Wireless LAN)

แนวทางการบริหารจัดการรหัสผ่าน

๒.๕.๑.๑ ผู้ดูและระบบ (Admin) เป็นผู้กำหนดรหัสผ่านสำหรับผู้ใช้งาน

๒.๕.๑.๒ ผู้ใช้งานที่สามารถ Login เข้าสู่ระบบ ต้องเป็นผู้ที่ศูนย์ข้อมูลและสารสนเทศอนุญาตเท่านั้น

๒.๕.๑.๓ รหัสผ่าน (Password) ที่ใช้สำหรับเข้าสู่ระบบถูกกำหนดโดยศูนย์ข้อมูลและสารสนเทศ

๒.๕.๑.๔ กำหนดการทบทวนสิทธิ/การยกเลิกรหัสผ่าน (Password) ผู้ดูแลระบบจะทำการทบทวนสิทธิและยกเลิกรหัสผ่าน (Password) / กรณีสมาชิกลาออก ตาย หรือย้ายสังกัดไปปฏิบัติงานหน่วยงานอื่นหรือ เป็นผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๒.๕.๑.๕ หากมีการฝ่าฝืนหรือกระทำความผิดจากสิทธิที่ได้รับต้องรับผิดตามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๒.๕.๒ ประเภทที่ ๒ เป็นระบบที่ให้บริการเครือข่ายสารสนเทศ เช่น ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบ Internet ระบบ Intranet และระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) เดิมที่มีการพัฒนาขึ้นและยังใช้งานอยู่จนถึงปัจจุบัน เช่น จดหมายอิเล็กทรอนิกส์ (E-Mail) ซึ่งระบบดังกล่าวถูกออกแบบและกำหนดให้ผู้ดูแลระบบ (Admin) เป็นผู้รับผิดชอบในการบันทึก/แก้ไข/ลบ ข้อมูลรหัสผู้ใช้งาน

แนวทางการบริหารจัดการรหัสผ่าน

๒.๕.๒.๑ ผู้ดูและระบบ (Admin) เป็นผู้กำหนดรหัสผ่าน (Password) สำหรับผู้ใช้งาน โดยจะทำการกำหนดสิทธิการใช้งานระบบและทำบันทึกโดยเจ้าหน้าที่ศูนย์ข้อมูลและสารสนเทศเป็นผู้ดำเนินการ

๒.๕.๒.๒ รหัสผ่าน (Password) ที่ใช้สำหรับเข้าสู่ระบบถูกกำหนดโดยศูนย์ข้อมูลและสารสนเทศ

๒.๕.๒.๓ กำหนดการทบทวนสิทธิ/การยกเลิกรหัสผ่าน (Password) ผู้ดูแลระบบจะทำการทบทวนสิทธิและยกเลิกรหัสผ่าน (Password) / กรณีสมาชิก ลาออก ตาย หรือย้ายสังกัดไปปฏิบัติงานองค์กรอื่น หรือ เป็นผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เป็นต้น

๒.๕.๒.๔ หากมีการฝ่าฝืน หรือกระทำความผิดจากสิทธิที่ได้รับต้องรับผิดตามตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

วิธีที่ ๒ การบริหารจัดการรหัสผ่านโดย ผู้ใช้งานสามารถแก้ไขได้ด้วยตนเอง

๒.๕.๓ ผู้ใช้งานสามารถแก้ไขได้ด้วยตนเอง

แนวทางการบริหารจัดการรหัสผ่าน

๒.๕.๓.๑ ผู้ดูและระบบ (Admin) เป็นผู้กำหนดรหัสผ่าน (Password) สำหรับผู้ใช้งาน โดยจะทำการกำหนดสิทธิ์การใช้งานระบบและทำบันทึกโดยเจ้าหน้าที่ศูนย์ข้อมูลและสารสนเทศ เป็นผู้ดำเนินการ

๒.๕.๓.๒ รหัสผ่าน (Password) ที่ใช้สำหรับเข้าสู่ระบบถูกกำหนดโดยศูนย์ข้อมูลและสารสนเทศ

๒.๕.๓.๓ ผู้ใช้งานสามารถแก้ไข/เปลี่ยนรหัสผ่าน (Password) ได้ด้วยตนเอง

๒.๕.๓.๔ ผู้ใช้ต้องรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและต้องปฏิบัติตามอย่างเคร่งครัด

๒.๕.๓.๕ ผู้ใช้งานที่ได้รับอนุญาตจะต้องรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศ และต้องปฏิบัติตามอย่างเคร่งครัด

๒.๖ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Rights)

แนวทางการทบทวนสิทธิ/ ยกเลิกสิทธิของผู้ใช้งานจากการเป็นสมาชิกระบบเครือข่ายของ สวพส.

๒.๖.๑ การทบทวนสิทธิการเข้าใช้งานของสมาชิกระบบเครือข่าย ผู้ดูแลระบบจะทำการทบทวนสิทธิ์ผู้ใช้งานส่วนบุคคล (Personal Account) อย่างน้อยปีละ ๑ ครั้ง

๒.๖.๒ ผู้ดูแลระบบจะทำการทบทวนสิทธิเมื่อมีการเปลี่ยนแปลงใดๆ เมื่อเปลี่ยนตำแหน่งงานภายในองค์กร ลดตำแหน่ง ย้ายตำแหน่ง หรือ สิ้นสุดการจ้างงาน หมดวาระ เกษียณอายุราชการ

๒.๖.๓ ผู้ดูแลระบบจะทำการยกเลิกสิทธิ เมื่อสมาชิก ลาออก ตาย หรือ ย้ายสังกัดไปปฏิบัติงานองค์กรอื่นหรือเป็นผู้กระทำผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๓. การควบคุมการเข้าถึงห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย (Server Room Control)

๓.๑ การปฏิบัติสำหรับผู้ดูแลระบบและเจ้าหน้าที่ มีดังนี้

๓.๑.๑ ผู้ดูแลระบบต้องตรวจสอบดูแลบุคคลที่มาติดต่อและขออนุญาตเข้ามาภายในห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายตลอดเวลาที่ปฏิบัติงานโดยเคร่งครัด

๓.๑.๒ ผู้ดูแลระบบ ต้องจัดทำทะเบียนผู้สิทธิเข้า-ออกห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย และกำหนดสิทธิในการเข้า-ออกห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายให้เฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายเท่านั้น

๓.๑.๓ เจ้าหน้าที่ทุกคนต้องทำบัตรผ่านเพื่อใช้ในการเข้า-ออกห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย

๓.๑.๔ เจ้าหน้าที่ต้องตรวจสอบอุปกรณ์ที่ผู้ติดต่อนำเข้า-ออกทุกครั้ง

๓.๑.๕ ต้องให้บุคคลที่ผ่านเข้า-ออกลงบันทึกตามแบบฟอร์ม “บันทึกการเข้า-ออกห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย”

๓.๒ การปฏิบัติสำหรับบุคคลภายนอก มีดังนี้

๓.๒.๑ ผู้ติดต่อจากภายนอกต้องได้รับอนุญาตจากหัวหน้าศูนย์ข้อมูลและสารเทศเท่านั้น จึงมีสิทธิในการเข้า-ออกห้องปฏิบัติการเครื่องแม่ข่าย

๓.๒.๒ กรณีที่นำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์แม่ข่ายต้องได้รับอนุญาตจากหัวหน้าศูนย์ข้อมูลและสารเทศ

๓.๒.๓ ผู้ติดต่อจากภายนอกต้องลงบันทึกในการบันทึกการเข้า-ออก ห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายให้ถูกต้องชัดเจน

๔. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

๔.๑ การควบคุมการติดตั้งซอฟต์แวร์

๔.๑.๑ การติดตั้งหรือปรับปรุงซอฟต์แวร์ต้องได้รับอนุญาตจากหัวหน้าศูนย์ข้อมูลและสารเทศทุกครั้ง และมีผู้ดูแลระบบดูแลตลอดการดำเนินการ

๔.๑.๒ มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศเพื่อป้องกันความเสียหายหรือการหยุดชะงัก

๔.๑.๓ มีการแจ้งให้ผู้ใช้งานที่เกี่ยวข้องได้รับทราบ หากจำเป็นต้องปิดระบบสารสนเทศหรือเครื่องคอมพิวเตอร์แม่ข่ายเพื่อปรับปรุง

๔.๑.๔ ต้องทำการทดสอบการทำงานของระบบสารสนเทศหรือซอฟต์แวร์อย่างเพียงพอและรัดกุม รวมทั้งทดสอบความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งลงบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๔.๒ การพัฒนาระบบสารสนเทศโดยผู้รับจ้างภายนอก

๔.๒.๑ มีการควบคุมโครงการพัฒนาระบบสารสนเทศโดยผู้รับจ้างภายนอก

๔.๒.๒ ต้องระบุผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับ Source Code ในการพัฒนาระบบสารสนเทศโดยผู้รับจ้างภายนอก

๔.๒.๓ ต้องตรวจสอบโปรแกรมชุดคำสั่งไม่พึงประสงค์ในซอฟต์แวร์ต่างๆ ก่อนทำการติดตั้งในเครื่องคอมพิวเตอร์แม่ข่าย

๔.๓ มาตรการควบคุมผู้ให้บริการภายนอก

๔.๓.๑ ผู้ให้บริการที่ต้องการสิทธิ์ในการเข้าถึงระบบสารสนเทศของสถาบันจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรจากหัวหน้าศูนย์ข้อมูลและสารเทศ

๔.๓.๒ ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบงานของผู้ให้บริการที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการว่าจ้างงานโดยทันทีหรือภายในระยะ เวลาที่กำหนดไว้

๔.๓.๓ ดำเนินการเพิกถอน ลบ หรือเปลี่ยนรหัสผ่านของผู้ให้บริการที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการว่าจ้างงานโดยทันทีหรือภายในระยะ เวลาที่กำหนดไว้

๔.๓.๔ กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงานเท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริงจะต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

๔.๓.๕ การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งไว้โดยไม่จำเป็น มีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว

๔.๔ การควบคุมช่องโหว่ทางเทคนิค

๔.๔.๑ ผู้ดูแลระบบต้องปรับปรุงโปรแกรมจัดการช่องโหว่ต่างๆ (Patch) อย่างสม่ำเสมอ

๔.๔.๒ ต้องมีการควบคุมพอร์ตที่ใช้ในการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายอย่างรอบคอบและรัดกุม โดยเปิดเฉพาะพอร์ตที่จำเป็นต้องใช้เท่านั้น

๔.๕ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) จัดให้มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

๔.๕.๑ ข้อมูลชื่อบัญชีผู้ใช้

๔.๕.๒ ข้อมูลวันเวลาที่เข้าถึงระบบ

๔.๕.๓ ข้อมูลวันเวลาที่ออกจากระบบ

๔.๕.๔ ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

๔.๕.๕ ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ

๔.๕.๖ ข้อมูลการพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

๔.๕.๗ ข้อมูลการเปลี่ยนค่าระบบ (Configuration)

๔.๕.๘ ข้อมูลการใช้งานแอพพลิเคชัน

๔.๕.๙ ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่าน

๔.๕.๑๐ ข้อมูลหมายเลขอุปกรณ์ (IP Address)

๔.๕.๑๑ ข้อมูลโปรโตคอลที่ใช้งาน

๕. การควบคุมการเข้าถึงระบบเครือข่าย (Network System Access Control)

การควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการเครือข่ายโดยไม่ได้รับอนุญาต โดยมีรายละเอียด ดังนี้

๕.๑ การใช้งานบริการเครือข่าย กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงแต่บริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๕.๑.๑ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

แนวทางการปฏิบัติ

๕.๑.๑.๑ ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ สวพส. จะต้องทำการลงทะเบียนกับศูนย์ข้อมูลและสารสนเทศ

๕.๑.๑.๒ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้งานระบบเครือข่ายไร้สายและมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งานเท่านั้น

๕.๑.๒ การบริหารจัดการการเข้าถึงระบบเครือข่าย

แนวทางการปฏิบัติ

๕.๑.๒.๑ ผู้ดูแลระบบ ออกแบบระบบเครือข่ายตามกลุ่มของผู้ใช้เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

๕.๑.๒.๒ การเข้าสู่ระบบเครือข่ายภายใน สวพส. โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบเทคโนโลยีสารสนเทศและการสื่อสารก่อนที่จะสามารถใช้งานได้ในทุกกรณี

๕.๑.๒.๓ ผู้ดูแลระบบ จำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๑.๓ การควบคุมการเข้าใช้งานระบบจากภายนอก

แนวทางการปฏิบัติ

๕.๑.๓.๑ การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของ สวพส. ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากร การควบคุมบุคคลที่เข้าสู่ระบบของสถาบันจากระยะไกล จึงกำหนดมาตรการ การรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๕.๑.๓.๒ วิธีการรูปแบบใดก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจากหัวหน้าศูนย์ข้อมูลและสารเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ รวมถึงผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ข้อมูลและระบบอย่างเคร่งครัด

๕.๑.๓.๓ ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสถาบันอย่างเพียงพอ

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User Authentication for External Connections) กำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

ขั้นตอนการปฏิบัติ

๕.๒.๑ ผู้ใช้งานจะมีชื่อและรหัสผ่านที่ถูกกำหนดให้ โดยเจ้าหน้าที่ที่รับผิดชอบงานด้านการควบคุม Access Control ของ สวพส.

๕.๒.๒ ทุกครั้งที่มีการใช้งาน ระบบจะร้องขอการพิสูจน์ตัวตนผ่าน login โดยจะต้องใช้ชื่อและรหัสผ่านในการเข้ามาใช้งานในระบบทุกครั้ง

๕.๒.๓ ระบบจะมีการบันทึกการเข้าใช้งานของ User ทุกคน เพื่อใช้ตรวจสอบในกรณีมีข้อสงสัยหรือเกิดปัญหา

๕.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) เป็นวิธีการที่จะสามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

ขั้นตอนการปฏิบัติ

๕.๓.๑ อุปกรณ์เครือข่ายทุกเครื่องจะมีการตรวจสอบ MAC Address จากนั้นทำการบันทึก MAC Address เข้ากับ IP Address ที่นำมาใช้งานและเก็บไว้ในระบบ

๕.๓.๒ ในการทำงานระบบจะตรวจสอบ IP Address อุปกรณ์เครือข่ายที่เชื่อมต่อเข้ามากับฐานข้อมูล MAC Address บันทึกเพื่อยืนยันและตรวจสอบตัวตนของอุปกรณ์ว่าเป็นอุปกรณ์เครือข่ายที่ถูกต้อง จากนั้นจะทำการบันทึกลง Log File

๕.๓.๓ จัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่ใช้เชื่อมกับระบบเครือข่ายของสถาบัน โดยมีรายละเอียดของอุปกรณ์ประกอบด้วย เครื่องคอมพิวเตอร์, IP Address, MAC Address, สถานที่ติดตั้ง, ผู้ใช้งาน เป็นต้น

๕.๓.๔ การติดตั้งเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์ข้อมูลและสารสนเทศหรือผู้ที่ได้รับอนุญาตเท่านั้น

๕.๓.๕ ต้องใช้ไฟร์วอลล์ (Firewall) กำหนดหมายเลขอุปกรณ์ที่สามารถเข้าถึงเครือข่ายของสถาบันได้

๕.๓.๖ จัดทำแผนผังระบบเครือข่าย ซึ่งประกอบด้วยรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก พร้อมทั้งอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

๕.๓.๗ ทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

๕.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

ขั้นตอนการปฏิบัติ

๕.๔.๑ มีการป้องกัน port มีการควบคุมการเข้าถึงผ่านทางเครือข่าย โดยระบบพิสูจน์ตัวตนผ่าน Radius Server ที่ต้องระบุ User และ Password ที่มีสิทธิเข้ามาใช้งาน

๕.๔.๒ การควบคุมการเข้าถึงทางกายภาพ มีการป้องกันผ่านระบบรักษาความปลอดภัยห้องระบบเครือข่าย โดยมีการติดตั้งอุปกรณ์ตรวจสอบในการเข้าออกพร้อมบันทึกประวัติทุกครั้ง

๕.๔.๓ มีการกำหนด password ในช่อง console ที่ใช้เชื่อมต่ออุปกรณ์เครือข่ายเพื่อพิสูจน์สิทธิ์การเรียกใช้งาน

๕.๔.๔ มีการป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย และเปิดใช้เฉพาะอุปกรณ์ที่จำเป็นเท่านั้น

๕.๔.๕ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่านั้น

๕.๔.๖ ติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

๕.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

ขั้นตอนการปฏิบัติ

๕.๕.๑ มีการแบ่งแยกเครือข่าย มีการบริหารผ่านทาง VLAN Management โดยกลุ่มงานของแต่ละหน่วยงานจะมีการจัดแบ่งอยู่คนละเครือข่าย

๕.๕.๒ มีการนำเอา Access List Control มาควบคุมการใช้งานของ IP Address ที่อยู่ในเครือข่ายเดียวกัน

๕.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

ขั้นตอนการปฏิบัติ

๕.๖.๑ มีการควบคุมการเชื่อมต่อทางเครือข่ายของ สวพส. ต่อหน่วยงานอื่น มีการใช้ Access Control Lists มาควบคุมการอนุญาตใช้งาน ผ่านทาง Protocol และ IP Address ในการให้สิทธิ์ Permission

๕.๖.๒ มีการควบคุมผ่านทางสิทธิ์ permission ของระบบปฏิบัติการ Windows

๕.๗ การเข้าถึงระบบเครือข่ายไร้สาย

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการ

ปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๕.๗.๑ ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ สวพส. จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยกรอกข้อมูลลงในแบบฟอร์มที่ศูนย์ข้อมูลและสารสนเทศกำหนด

๕.๗.๒ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๕.๗.๓ ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สายลงในแบบฟอร์ม

๕.๗.๓ ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (default) มาจากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน

๕.๗.๔ ผู้ดูแลระบบควรเปลี่ยนค่าชื่อ login และ Password สำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อ login และ Password ที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๕.๗.๕ ผู้ดูแลระบบต้องกำหนดค่า WEP หรือ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ Access Point เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

๕.๗.๖ ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address และชื่อผู้ใช้ รหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

๕.๘ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

แนวปฏิบัติในการจัดเส้นทางบนเครือข่าย ดังนี้

๕.๘.๑ ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๕.๘.๒ ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๕.๘.๓ กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก

๕.๘.๔ ต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต มีรายละเอียด ดังนี้

๖.๑ การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยการเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

แนวทางการปฏิบัติ

๖.๑.๑ มีการกำหนดรหัสผ่านในฐานข้อมูล Bios เพื่อระบุสิทธิที่ถูกต้องของการเข้าใช้งาน

๖.๑.๒ มีการกำหนด Username และ Password ที่เครื่องแม่ข่าย Domain Controller โดยเจ้าหน้าที่ Admin ที่ดูแลระบบ

๖.๑.๓ ในการเรียกใช้งานระบบปฏิบัติการจะมีหน้าต่างการ Login ซึ่งผู้ใช้งานจะต้องกรอก User และ Password ในการเข้าใช้งานทุกครั้ง จากนั้นระบบจะให้สิทธิ์ Permission ตาม Login ที่เข้ามา

๖.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) กำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

แนวทางการปฏิบัติ

๖.๒.๑ มีการกำหนด User name และ Password ที่เครื่องแม่ข่าย Domain Controller โดยเจ้าหน้าที่ Admin ที่ดูแลระบบ

๖.๒.๒ ในการเรียกใช้งานระบบปฏิบัติการจะมีหน้าต่างการ Login ซึ่งผู้ใช้งานจะต้องระบบ User และ Password ในการเข้าใช้งานทุกครั้ง จากนั้นระบบจะให้สิทธิ์ Permission ตาม Login ที่เข้ามา

๖.๓ การบริหารจัดการรหัสผ่าน (Password Management System)

แนวทางการปฏิบัติ

๖.๓.๑ มีการบริหารจัดการรหัสผ่าน เพื่อระบุและยืนยันการเข้าใช้งานโดยใช้ชื่อ (User name) และรหัสผ่าน (Password) ที่มีการเข้ารหัส

๖.๓.๒ การกำหนดคุณลักษณะที่ดีของรหัสผ่าน ต้องตรงตามมาตรฐานการรักษาความปลอดภัยของระบบปฏิบัติการ

๖.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) จำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

แนวทางการปฏิบัติ

๖.๔.๑ ผู้ดูแลระบบ จัดทำบัญชีรายชื่อโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งานได้เท่านั้น

๖.๔.๒ ผู้ใช้งานที่ต้องการใช้งานโปรแกรมอรรถประโยชน์ ต้องแจ้งความจำเป็นในการขอใช้และทำการขออนุญาตจากผู้ดูแลระบบ พร้อมระบุเหตุผลความต้องการใช้งาน

๖.๔.๓ ผู้ดูแลระบบ กำหนดสิทธิ์อนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไปและมีการเก็บบันทึกการเรียกใช้งานโปรแกรมอรรถประโยชน์ทุกครั้ง แม้จะเป็นการใช้งานเพียงชั่วคราว ก็จำเป็นต้องทำการขออนุมัติการใช้งานโปรแกรมอรรถประโยชน์ ทุกครั้ง

๖.๔.๔ ผู้ดูแลระบบต้องทำการตรวจสอบบันทึกการเรียกใช้งานอย่างสม่ำเสมอ

๖.๔.๕ ผู้ดูแลระบบต้องกำหนดให้มีการยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์ที่ไม่มีความจำเป็นในการใช้งานแล้ว

๖.๔.๖ ซอฟต์แวร์ที่สถาบันใช้มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานซอฟต์แวร์ได้ตามหน้าที่ความจำเป็น

๖.๔.๗ ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

๖.๔.๘ ห้ามผู้ใช้ทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือคัดลอกโปรแกรมไปใช้ผิดวัตถุประสงค์องค์กร

๖.๕ การกำหนดระยะเวลาให้ยุติการใช้งานระบบสารสนเทศ (Session Time-Out) เมื่อมีการว่างจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out)

แนวทางการปฏิบัติ

๖.๕.๑ เมื่อไม่มีการเรียกใช้งานในเวลาที่กำหนด ระบบปฏิบัติการจะมีการเข้าสู่ idle mode เพื่อพักการใช้งาน

๖.๕.๒ เมื่อผู้ใช้งานต้องการเรียกกลับเข้ามาใช้งานใหม่ จะมีหน้าต่าง Login เพื่อให้ระบุ User และ Password ในการเข้ามาใช้งานพร้อมทั้งบันทึกประวัติ Login เพื่อใช้ในการตรวจสอบ

๖.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

แนวทางการปฏิบัติ

๖.๖.๑ เมื่อมีการเชื่อมต่อเข้ามาในระบบจากภายนอก จะต้องมีการระบุรหัสผ่าน Username และ Password ที่ทางสถาบันกำหนด (มีการเข้ารหัสข้อมูลก่อน) จากนั้นถ้าข้อมูลถูกต้อง ระบบจะสร้าง Session เข้ามาเชื่อมโยงและบันทึกเวลาการเข้าเชื่อมต่อ

๖.๖.๒ การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๖.๖.๓ กำหนดให้ระบบสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อไม่เกิน ๓ ชั่วโมงต่อครั้ง

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๗.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าไปใช้งานของผู้ใช้และบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

แนวทางการปฏิบัติ

๗.๑.๑ มีการกำหนด Username และ Password สำหรับการเข้าถึงหรือเข้าไปใช้งานของผู้ใช้และบุคลากรฝ่ายสนับสนุนเข้าใช้งานระบบโปรแกรมประยุกต์และสารสนเทศโดยเจ้าหน้าที่ admin ที่ดูแลระบบจะเป็นผู้กำหนดให้

๗.๑.๒ ในการเรียกใช้งานระบบโปรแกรมประยุกต์และสารสนเทศ จะมีหน้าต่าง Login ซึ่งผู้ใช้งานจะต้องระบุ User และ Password ก่อนการเข้าใช้งานทุกครั้ง จากนั้นระบบจะให้สิทธิ์ Permission ในการเข้าถึงฟังก์ชั่น (Functions) ต่างๆ ของระบบซึ่งจะแตกต่างกันตามสิทธิ์ของ Login

๗.๑.๓ จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่างๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด โดยยกเลิกการเชื่อมต่อระบบเมื่อครบกำหนดเวลา

๗.๑.๔ ผู้ให้บริการภายนอก (Outsource) ต้องทำความเข้าใจกับนโยบายความมั่นคงปลอดภัยของสถาบัน และต้องลงนามในสัญญาการรักษาความลับและไม่เปิดเผยข้อมูลของสถาบัน

๗.๑.๕ ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

๗.๑.๖ ผู้ดูแลระบบต้องควบคุม การเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource)ให้มีสิทธิเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource)

๗.๒ การแยกระบบสารสนเทศที่มีผลกระทบและความสำคัญสูงต่อสถาบัน ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสถาบัน ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเอง โดยเฉพาะให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่ รวมถึงการปฏิบัติงานจากภายนอกสถาบัน (Mobile Computing and Teleworking)

แนวทางการปฏิบัติ

๗.๒.๑ การจำกัดการเข้าถึงสารสนเทศและควบคุมการเข้าใช้งานทางด้านกายภาพ โดยแยกระบบที่มีความสำคัญมาเก็บรักษาไว้ในห้องควบคุมระบบที่มีระบบรักษาความปลอดภัย ในการเข้าออกห้องทุกครั้งจะต้องได้รับอนุญาตผ่านอุปกรณ์ที่ติดตั้งไว้ ซึ่งจะให้อนุญาตเฉพาะผู้ที่มีสิทธิ์ในการเข้าถึงเท่านั้น

๗.๒.๒ การจำกัดการเข้าถึงสารสนเทศและควบคุมการเข้าใช้งานจากระบบเครือข่าย โดยการจำกัดสิทธิ์ ผู้ใช้งานที่สามารถเข้ามาใช้งานให้มีสิทธิ์ในการอ่านเพียงอย่างเดียว และเฉพาะบุคคลที่มีความเกี่ยวข้องกับโปรแกรมดังกล่าวเท่านั้น

๗.๒.๓ ผู้ใช้งานไม่สามารถ Remote ผ่านทางการ Login มาจากเครือข่ายภายนอกสถาบันหรือเครือข่ายไร้สายที่ให้บริการสำหรับบุคคลภายนอกของสถาบันได้หากไม่ได้รับอนุญาต

๗.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ กำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

แนวทางการปฏิบัติ

๗.๓.๑ มีการควบคุมเครือข่ายไร้สายที่ให้บริการโดยการควบคุม MAC Address ของคอมพิวเตอร์ที่มีสิทธิ์เข้าใช้งาน

๗.๓.๒ เมื่อผู้ใช้งานที่มีสิทธิ์ในการเรียกใช้งาน จะต้องเรียกใช้งานผ่านการ Login และใช้รหัสผ่านที่มีการเข้ารหัส ซึ่งถูกกำหนดโดยเจ้าหน้าที่ Admin ที่ดูแลระบบและผู้ใช้งานที่ทำการ Login เข้ามาจะมี Permission ในการมาใช้งานแตกต่างกันตามสถานะที่ผู้ดูแลระบบกำหนด

๗.๔ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) กำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

แนวทางการปฏิบัติ

๗.๔.๑ เจ้าหน้าที่ Admin ที่ดูแลระบบจะกำหนด Username และ Password ไว้ในเครื่อง Radius ที่ให้บริการ โดยในแต่ละ User จะมี Permission ในการเข้ามาใช้งานแตกต่างกัน

๗.๔.๒ การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัวต้องได้รับอนุญาตจากหัวหน้าศูนย์ข้อมูลและสารสนเทศ

๗.๔.๓ ไม่อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานสำหรับระบบงานที่มีความลับในระดับชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด

๗.๔.๔ ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

๗.๔.๕ ผู้ดูแลระบบจะทำการยกเลิกสิทธิการเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกหน่วยงาน แก่ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อหัวหน้าศูนย์ข้อมูลและสารสนเทศ

๗.๔.๖ ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอก หน่วยงานอย่างน้อยปีละ 1 ครั้ง

๘. การควบคุมการใช้งานอินเทอร์เน็ต

เพื่อควบคุมการใช้งานอินเทอร์เน็ตภายในสถาบันอย่างปลอดภัย

แนวทางปฏิบัติการใช้งานอินเทอร์เน็ต

๘.๑ ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่สถาบันจัดสรรไว้เท่านั้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากหัวหน้าศูนย์ข้อมูลและสารสนเทศเป็นลายลักษณ์อักษร

๘.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บเบราเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ

๘.๓ การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๘.๔ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็น การส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรมเว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับสถาบัน

๘.๕ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสถาบันที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

๘.๖ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต (Internet) การอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

๘.๗ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์จะต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสถาบัน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๘.๘ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๘.๙ หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์ (Web Browser)และออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๘.๑๐ ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

๘.๑๑ ห้ามผู้ใช้งาน ใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมากหรือเป็นเวลานาน

๙. การควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ผ่านระบบเครือข่ายของสถาบัน ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์

ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๙.๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของสถาบันให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การย้ายสำนัก เป็นต้น

๙.๒ ผู้ใช้รายใหม่ที่ต้องการขอลงทะเบียนบัญชีชื่อผู้ใช้ ต้องทำการกรอกข้อมูลคำขอลงในแบบฟอร์มที่สถาบันกำหนด และยื่นคำขอกับเจ้าหน้าที่ผู้ดูแลระบบเพื่อดำเนินการกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน

๙.๓ ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของสถาบัน

๙.๔ ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๙.๕ ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อสถาบันหรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่นหรือผิดกฎหมาย หรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของสถาบัน

๙.๖ ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่าน รับ-ส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๙.๗ ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของสถาบันเพื่อการทำงานของสถาบันเท่านั้น

๙.๘ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๘.๙ ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

๙.๑๐ ผู้ใช้ไม่ควรเปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๙.๑๑ ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของสถาบัน ทำให้เกิดความแตกแยกระหว่างสถาบันผ่านทางจดหมายอิเล็กทรอนิกส์

๙.๑๒ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๙.๑๓ ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๙.๑๔ ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๙.๑๕ ผู้ใช้ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

๙.๑๖ ผู้ใช้ควรทำการสำรองข้อมูลในจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอเลือกสำรองจดหมายอิเล็กทรอนิกส์ที่มีความสำคัญมาก โดยอาจทำการส่งต่อไปยังจดหมายอิเล็กทรอนิกส์แอดเดรสอื่น หรือทำการสำรองไว้ที่เมล์เซิร์ฟเวอร์ของสถาบัน

๙.๑๗ ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ ควรให้ความรู้เกี่ยวกับการรักษาความปลอดภัยในจดหมายอิเล็กทรอนิกส์แก่ผู้ใช้งานจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอ การให้ความรู้ถือเป็นการป้องกันเบื้องต้นเพื่อมิให้ผู้ใช้งานตกเป็นเหยื่อของผู้ไม่หวังดี และเป็นการป้องกันไม่ให้เกิดปัญหา ในกรณีที่ทำผิดพลาดแม้เพียงครั้งเดียว อาจส่งผลกระทบทำให้ระบบไม่สามารถทำงานได้

๙.๑๘ ในการใช้จดหมายอิเล็กทรอนิกส์ในการติดต่อสื่อสารนั้น ผู้ใช้ควรให้เกียรติกับผู้รับปลายทางเหมือนการสนทนาด้วยวาจา ควรตรวจสอบตัวสะกดไวยากรณ์ อ่านทวนเนื้อหาก่อนส่ง ใช้ข้อความที่กระชับเข้าถึงประเด็นอย่างรวดเร็ว แต่ข้อความต้องไม่สั้นเกินจนดูแล้วห้วน และให้ตระหนักอยู่เสมอว่าข้อความใดๆ ที่ส่งผ่านเครือข่ายอินเทอร์เน็ตนั้นเป็นข้อความที่สามารถมองเห็นและอ่านได้โดยผู้อื่น ดังนั้นการส่งข้อความที่เป็นความลับจะต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อเข้ารหัสข้อมูลนั้นก่อนส่งออกไป

๙.๑๙ ผู้ใช้ต้องไม่ทำการเปลี่ยนแปลง หรือแก้ไขข้อความจดหมายอิเล็กทรอนิกส์ต้นฉบับที่ได้รับมาและต้องการส่งต่อไป หากจดหมายอิเล็กทรอนิกส์นั้นถูกส่งถึง

ผู้รับเป็นการส่วนตัวต้องขออนุญาต ผู้ส่งก่อนที่จะส่งต่อจดหมายอิเล็กทรอนิกส์นั้นไปจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลส่วนบุคคลควรได้รับการเข้ารหัสอย่างปลอดภัย (Encryption)

๙.๒๐ ผู้ใช้ควรใส่ชื่อหัวข้อเรื่องใน Subject ของจดหมายอิเล็กทรอนิกส์ เพื่อแสดงถึงเรื่องของจดหมายอิเล็กทรอนิกส์ที่ต้องการหารือหรือแจ้งให้ทราบ และควรส่งจดหมายอิเล็กทรอนิกส์ตอบกลับสั้นๆ หากไม่มีเวลาพอเพื่อให้ผู้ส่งได้รับทราบว่าผู้รับได้รับจดหมายอิเล็กทรอนิกส์นั้นแล้วและจะตอบกลับอย่างสมบูรณ์ในภายหลัง

๙.๒๑ ผู้ใช้ไม่ควรส่งต่อจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งที่ไม่สมควรทำบนเครือข่ายอินเทอร์เน็ต หากได้รับจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ และมีข้อความขอให้ส่งต่อจดหมายอิเล็กทรอนิกส์นั้นให้ติดต่อหรือแจ้งผู้ดูแลระบบโดยทันที

๙.๒๒ ผู้ใช้ไม่ควรส่งจดหมายอิเล็กทรอนิกส์ที่เกี่ยวกับการล่วงละเมิดหรือข่มขู่ หรือมีเนื้อหาข้อความที่ขัดต่อกฎหมายและศีลธรรม และใช้จดหมายอิเล็กทรอนิกส์เป็นเครื่องมือในการกระจายข่าวสาร เว้นแต่เป็นการประกาศที่เหมาะสม

๙.๒๓ ผู้ใช้ควรพิจารณาใช้ “BCC” (Blind Carbon Copy - สำเนาโดยที่ผู้รับไม่ทราบ) ในการส่งจดหมายอิเล็กทรอนิกส์ถึงผู้รับเป็นจำนวนมากเพื่อไม่ให้รายชื่อผู้รับทั้งหมดปรากฏในลักษณะที่ยาวมากเกินไป

๙.๒๔ ผู้ใช้ควรทำตามนโยบายอย่างเคร่งครัด และแจ้งผู้ดูแลระบบเมื่อพบการใช้จดหมายอิเล็กทรอนิกส์ที่ไม่ถูกต้อง

๙.๒๕ ผู้ใช้จะต้องกรอกข้อมูลในช่องข้อมูลส่วนตัว (identity) โดยจะต้องใช้ชื่อผู้ส่ง (Sender) ที่เป็นจริง ตามที่มีบัญชีรายชื่ออยู่จริง เพื่อให้สามารถอ้างอิงในกรณีที่มีปัญหาเกิดขึ้น

๙.๒๖ ผู้ใช้ต้องไม่ตั้งชื่อผู้ส่ง (Sender) หรือข้อมูลอื่น ในลักษณะที่ส่อว่าเป็นผู้ดูแลระบบ administrator) เช่น Webmaster, Host Master, Administrator, Postmaster เป็นต้น โดยไม่ได้รับอนุญาต

๙.๒๗ ผู้ใช้ต้องไม่ทำการส่งจดหมายอิเล็กทรอนิกส์ในลักษณะของจดหมายลูกโซ่ จดหมายชี้ชวน หรือ อื่นๆ อันเป็นการกระทำที่เข้าข่าย Spam หรือ Unsolicited Electronic Mail อย่างเด็ดขาด

๙.๒๘ ผู้ใช้บริการมีหน้าที่ต้องรักษาชื่อผู้ใช้และรหัสผ่านเป็นความลับ ไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๙.๒๙ จดหมายของผู้ใช้บริการ ถือเป็นข้อมูลส่วนบุคคล ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ไม่สามารถจะทำการเก็บ กู้ หรือ ดึงข้อมูลส่วนตัวขึ้นมาได้ ดังนั้นผู้ใช้บริการจะต้องดูแลรักษาข้อมูลดังกล่าวอย่างระมัดระวัง โดยเฉพาะการลบจดหมายที่ไม่ต้องการ รวมทั้งจะต้องดูแลรักษาไม่ให้ขนาดของจดหมายที่จัดเก็บเกินกว่าจำนวนพื้นที่ที่ได้รับอนุญาต

๙.๓๐ ผู้ใช้ต้องมีความรับผิดชอบ และระมัดระวังในการใช้บริการตามสมควร ไม่ให้ล่วงละเมิดบุคคลอื่น รวมถึงศีลธรรม หรือกฎหมายใดๆ อันเป็นผลให้เกิดความไม่สงบเรียบร้อยในสถาบันและสังคมถูกต้อง

๑๐. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการดูแลปกป้องอุปกรณ์สารสนเทศให้ปลอดภัย

๑๐.๑ การใช้งานรหัสผ่าน (Password Use) แนวปฏิบัติที่ดีสาหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ให้ผู้ใช้งานปฏิบัติ ดังนี้

๑๐.๑.๑ เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอิน (Log in) เข้าใช้งานระบบเป็น ครั้งแรก

๑๐.๑.๒ ควรตั้งรหัสผ่านที่ยากต่อการคาดเดา

๑๐.๑.๓ ควรกำหนดรหัสผ่านให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ 8 ตัว**อักษร โดย**มีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๑๐.๑.๔ ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

๑๐.๑.๕ ไม่ตั้งรหัสผ่านโดยใช้ตัวเลขหรือตัวอักษรที่เรียงกันหรือเหมือนกันทั้งหมด หรือเป็นกลุ่มเหมือนกัน

๑๐.๑.๖ ไม่ใช้รหัสผ่านส่วนบุคคลสาหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

๑๐.๑.๗ เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

๑๐.๑.๘ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นหรือเก็บไว้ในคอมพิวเตอร์

๑๐.๑.๙ ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

๑๐.๑.๑๐ ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

๑๐.๑.๑๑ ไม่เปิดเผยรหัสผ่านให้คนอื่นรับทราบหรือใช้งานแทน กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้เปลี่ยนรหัสผ่านโดยทันที

๑๐.๑.๑๒ ควรเปลี่ยนรหัสผ่านอย่างน้อยทุก ๖ เดือน หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

๑๐.๑.๑๓ หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ของผู้ใช้งาน

๑๐.๑.๑๔ หลีกเลี่ยงการใช้รหัสผ่านเดิมเมื่อเปลี่ยนรหัสผ่านใหม่

๑๐.๑.๑๕ ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๑ เดือน

๑๐.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

แนวปฏิบัติที่เหมาะสม ดังนี้

๑๐.๒.๑ ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๑๐.๒.๒ ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอหลังจากที่ไม่ได้ใช้งาน เช่น ตั้งเวลาเป็น 15 นาที เป็นต้น และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๑๐.๒.๓ ผู้ใช้งานต้องล็อกใส่รหัสผ่านป้องกันการเข้าถึงอุปกรณ์ และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๑๐.๒.๔ ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์และสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด

๑๐.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน โดยมีแนวปฏิบัติผู้ใช้งาน ดังนี้

๑๐.๓.๑ กำหนดมาตรการป้องกันทรัพย์สินขององค์กรและควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย

๑๐.๓.๒ นำสินทรัพย์สารสนเทศที่มีความสำคัญมาก จัดเก็บรักษาไว้ในห้องควบคุมระบบที่มีระบบรักษาความปลอดภัย โดยในการเข้า-ออก ห้องทุกครั้งจะต้องสแกนลายนิ้วมือ โดยอนุญาตเฉพาะผู้ที่มีสิทธิ์ในการเข้าถึง

๑๐.๓.๓ มีการล็อคกุญแจตู้ที่เก็บรักษาสินทรัพย์และอนุญาตให้เฉพาะผู้มีหน้าที่เกี่ยวข้องเก็บรักษาลูกกุญแจไว้ โดยในการนำสินทรัพย์สารสนเทศออกมาใช้งานทุกครั้งจะต้องได้รับอนุญาตโดยผู้มีอำนาจ

๑๐.๓.๔ การจำกัดสิทธิ์ user ที่สามารถ login เข้ามาใช้งานเฉพาะบุคคลที่มีความเกี่ยวข้องกับสินทรัพย์สารสนเทศดังกล่าว และเมื่อไม่มีการเรียกใช้งานในเวลาที่กำหนด ระบบจะทำการ Logoff User นั้นออกโดยอัตโนมัติ

๑๐.๓.๕ การทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลาย ดังนี้

ลำดับ	ประเภทสื่อบันทึกข้อมูล	แนวทางการทำลาย
๑	แฟลชไดรฟ์ (Flash Drive) ฮาร์ดิสก์ (Hard disk) เอ็กเทอนอลฮาร์ดดิสก์ (External Hard disk)	๑ ทำลายข้อมูลตามแนวทางของ DOD ๕๒๒๐.๒๒-M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อูลโดยการเขียนทับข้อมูลเดิมหลายๆ รอบ ๒ ทุบทำลาย หรือบดให้อุปกรณ์เสียหายไม่

		สามารถนำไปใช้งานได้
๒	แผ่นซีดี / ดีวีดี (CD/DVD)	ใช้วิธีการตัด เผา ทำให้สิ้นสภาพการใช้งาน
๓	เทป	ใช้วิธีทุบ ทำลายให้เสียหายสิ้นสภาพการใช้งาน
๔	กระดาษ	ตัดด้วยเครื่องทำลายเอกสาร

๑๐.๔ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 โดยการรับ-ส่งข้อมูลสาคัญ หรือข้อมูลซึ่งเป็นความลับให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล SSL หรือ VPN

๑๑. การใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์

เพื่อให้ผู้ใช้ที่อยู่ภายในสถาบัน สามารถใช้บริการเครือข่ายภายในได้เต็มที่และใช้บริการเครือข่ายภายนอก เช่น อินเทอร์เน็ตได้ ในขณะที่ไฟร์วอลล์จะป้องกันไม่ให้ผู้ใช้ภายนอกเข้ามาใช้บริการเครือข่ายที่อยู่ภายใน ไฟร์วอลล์สามารถควบคุมการใช้เครือข่ายได้ โดยอนุญาตหรือไม่อนุญาตให้แพ็กเก็ตผ่านได้ซึ่งแพ็กเก็ตที่อนุญาตให้ผ่านหรือไม่ ขึ้นอยู่กับนโยบายการรักษาความปลอดภัย (Security Policy) ของเครือข่าย ไฟร์วอลล์เป็นระบบที่บังคับใช้นโยบายการรักษาความปลอดภัยระหว่างเครือข่าย โดยหลักการแล้วไฟร์วอลล์จะทำงานอยู่ ๒ กลไก คือ การอนุญาตหรือไม่อนุญาตให้แพ็กเก็ตผ่าน ถ้าเครือข่ายสถาบันมีการเชื่อมต่อโดยตรงกับอินเทอร์เน็ตโดยที่ไม่มีไฟร์วอลล์เป็นการเปิดช่องโหว่ให้เครือข่ายสามารถถูกโจมตีหรือบุกรุกได้อย่างง่ายดาย การติดตั้งไฟร์วอลล์จะเป็นการป้องกันผู้บุกรุกได้ในระดับหนึ่ง

แนวปฏิบัติการใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์ (Firewall) ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๑๑.๑ ผู้ดูแลระบบต้องเฝ้าระวังและบริหารจัดการระบบรักษาความปลอดภัย

๑๑.๒ ผู้ดูแลระบบต้องกำหนดนโยบายการใช้งานไฟร์วอลล์

๑๑.๓ ผู้ดูแลระบบต้องจัดให้มีระบบตรวจสอบตัวตนจริง และสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น การกำหนดรหัสผ่านให้ยากแก่การคาดเดา เป็นต้น

๑๑.๔ ผู้ดูแลระบบต้องกำหนดค่า (Configuration) หรือกำหนดนโยบาย (Policy) เพื่อกลั่นกรองข้อมูลที่มาทางเว็บไซต์ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) ป้องกันผู้บุกรุก ไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์

๑๑.๕ ผู้ดูแลระบบต้องกำหนดขั้นตอนหรือวิธีปฏิบัติ ในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติต้องดำเนินการแก้ไข

๑๑.๖ การเปิดใช้บริการ (Service) ต้องได้รับอนุญาตจากหัวหน้างานที่รับผิดชอบด้านสารสนเทศ ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ผู้ดูแลระบบต้องกำหนดมาตรการป้องกันเพิ่มเติม

๑๑.๗ ผู้ดูแลระบบต้องเปิดใช้งานไฟร์วอลล์ตลอดเวลา

๑๑.๘ ผู้ดูแลระบบต้องออกจากระบบงาน (Logout) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์

๑๑.๙ ผู้ดูแลระบบต้องกำหนดให้มีการควบคุมการใช้งาน โดยการจัดให้มีบัญชีผู้ใช้งาน

๑๑.๑๐ ผู้ดูแลระบบต้องบันทึกชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเป็นการตรวจสอบผู้ใช้ก่อนเข้าใช้งานระบบ (Authentication) และควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึงล่วงรู้ (Access Risk) หรือแก้ไข เปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง

๑๑.๑๑ ผู้ดูแลระบบต้องติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่างๆ ของซอฟต์แวร์ระบบ (System Software) เช่น ระบบปฏิบัติการ DBMS Web Server เป็นต้น อย่างสม่ำเสมอ

๑๑.๑๒ ผู้ดูแลระบบต้องทดสอบซอฟต์แวร์ระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังการแก้ไขหรือบำรุงรักษา

๑๑.๑๓ หัวหน้างานที่รับผิดชอบด้านสารสนเทศต้องกำหนดบุคคลรับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ อย่างชัดเจน

๑๑.๑๔ ผู้ขอใช้งานต้องยอมรับและปฏิบัติตามนโยบายด้านความปลอดภัยอย่างเคร่งครัด

๑๑.๑๕ วัตถุประสงค์ในการขอใช้งานจะต้องไม่ขัดต่อนโยบาย ประกาศ ระเบียบต่างๆ ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) และต่อกฎหมายที่เกี่ยวข้อง

๑๑.๑๖ ผู้ขอใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษร ต่อหัวหน้างานที่รับผิดชอบด้านสารสนเทศโดยระบุข้อมูลดังนี้

๑๑.๑๖.๑ หมายเลข Port ที่ต้องการขอให้เปิด

๑๑.๑๖.๒ หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

๑๑.๑๖.๓ วัตถุประสงค์หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port

๑๑.๑๖.๔ วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้

๑๑.๑๗ ในการขอใช้งานหากพบว่าการขัดต่อนโยบาย ประกาศ ระเบียบของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) หรือกฎหมาย หรืออาจทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ ศูนย์ข้อมูลและสารสนเทศจะไม่อนุญาตให้ใช้งาน

๑๑.๑๘ ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อ นโยบายประกาศ ระเบียบ ของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) หรือกฎหมาย หรืออาจจะทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศขององค์กร ศูนย์ข้อมูลและสารสนเทศ จะยกเลิกการให้บริการทันที และผู้ใช้งานจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๑๑.๑๙ ผู้ดูแลระบบต้องกำหนดแนวทางปฏิบัติในการใช้งาน software utility เช่น personal firewall password cracker เป็นต้น และตรวจสอบการใช้งาน software utility อย่างสม่ำเสมอ

๑๒. การสร้างความมั่นคงปลอดภัยด้านกายภาพและสิ่งแวดล้อม

เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพที่เกี่ยวข้องกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลสารสนเทศซึ่งเป็นทรัพย์สินของสถาบัน

๑๒.๑ แนวปฏิบัติการสร้างความมั่นคงปลอดภัยด้านกายภาพและสิ่งแวดล้อม

๑๒.๑.๑ กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารให้ชัดเจนและจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๑๒.๑.๒ มีการรักษาความมั่นคงปลอดภัยให้กับพื้นที่ที่ใช้ในการติดตั้ง จัดเก็บ หรือใช้งานระบบและข้อมูลสารสนเทศ

๑๒.๑.๓ มีการออกแบบแนวทางป้องกันทางด้านกายภาพและสภาพแวดล้อมสำหรับการทำงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม และต้องกำหนดให้มีการนำไปใช้งานจริง

๑๒.๑.๔ จัดวางและป้องกันอุปกรณ์สารสนเทศ เพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่างๆ และเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๑๒.๑.๕ มีการป้องกันอุปกรณ์สารสนเทศที่อาจเกิดความเสียหายจากไฟฟ้าขัดข้องหรือที่อาจหยุดชะงักจากข้อผิดพลาดของโครงสร้างพื้นฐาน

๑๒.๑.๖ มีการดูแลอุปกรณ์สารสนเทศอย่างถูกวิธี เพื่อให้ข้อมูลสารสนเทศมีความถูกต้องครบถ้วนและอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ

๑๒.๑.๗ ไม่นำอุปกรณ์สารสนเทศ ข้อมูลสารสนเทศ หรือซอฟต์แวร์ออกจากสถานที่ปฏิบัติงานของสถาบันวิจัยและพัฒนาพื้นที่สูง (องค์การมหาชน) หากไม่ได้รับอนุญาต

๑๒.๑.๘ ในพื้นที่ที่มีการรักษาความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม ต้องมีการควบคุมการเข้า-ออก โดยจะกำหนดให้ผู้ที่มีสิทธิ์เท่านั้นที่สามารถเข้า-ออกพื้นที่ได้

๑๒.๒ การรักษาความมั่นคงปลอดภัยทางกายภาพ

๑๒.๒.๑ หัวหน้างานที่รับผิดชอบด้านสารสนเทศหรือเจ้าหน้าที่ที่ได้รับมอบหมายเป็นผู้กำหนดรายละเอียดของขอบเขตสถานที่และอุปกรณ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันความเสียหายและควบคุมการเข้า-ออก ในเขตรักษาความปลอดภัยให้เหมาะสมกับสถานที่หรือพื้นที่ที่ต้องรักษาความปลอดภัยอย่างเหมาะสม

๑๒.๒.๒ จะต้องจัดให้มีการควบคุมการเข้า-ออก ในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัยและอนุญาตให้ผ่านเข้า-ออก ได้เฉพาะผู้ที่ได้รับอนุญาตแล้วเท่านั้น

๑๒.๒.๓ เจ้าหน้าที่และผู้ปฏิบัติงานจะต้องไม่เปิดประตูห้อง Server ทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่โดยเด็ดขาด เพื่อป้องกันการเข้าถึงพื้นที่ห้อง Server หรือพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

๑๒.๒.๔ ต้องจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยอื่นๆ ให้แก่สถาบัน ห้องทำงานและเครื่องมือต่างๆ อาทิ เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงโดยไม่ตั้งอยู่ในบริเวณที่มีการผ่าน เข้า-ออก ของบุคคลจำนวนมาก

๑๒.๒.๕ จัดให้มีระบบการควบคุมความปลอดภัยของห้อง Server อาทิ เครื่องอ่านบัตร เครื่องสแกนลายนิ้วมือ หรือกล้องโทรทัศน์วงจรปิด

๑๒.๓ ความมั่นคงปลอดภัยของอุปกรณ์เทคโนโลยีสารสนเทศ

๑๒.๓.๑ มีการกำหนดหน้าที่ของอุปกรณ์รวมถึงการพิจารณาคัดเลือกความเหมาะสมของอุปกรณ์ที่นำมาใช้สำหรับสำรองข้อมูลเพื่อให้เพียงพอและสามารถรองรับปริมาณข้อมูลปัจจุบันและรวมถึงอนาคต

๑๒.๓.๒ จัดให้มีแผนสำรองของอุปกรณ์ต่างๆ ในกรณีฉุกเฉินหรือกรณีที่อุปกรณ์ได้รับความเสียหายอันเกิดจากเหตุการณ์ที่คาดไม่ถึง โดยเฉพาะอุปกรณ์ที่มีความจำเป็นและสำคัญต่อการปฏิบัติงาน อาทิ เครื่องสำรองไฟ เป็นต้น

๑๒.๓.๓ จัดให้มีแผนการบำรุงรักษาอุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ได้ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

๑๒.๓.๔ จัดแผนป้องกันรักษาข้อมูลที่จัดเก็บอยู่ในอุปกรณ์บันทึกข้อมูลหรือระบบคอมพิวเตอร์ มิให้ข้อมูลที่จัดเก็บเกิดความรั่วไหล กรณีที่มีความจำเป็นต้องเคลื่อนย้ายอุปกรณ์ไปยังสถานที่เก็บแห่งใหม่ หรือนำเอาอุปกรณ์ไปซ่อมบำรุงหรือชำรุด

ส่วนที่ ๒
นโยบายการจัดทำระบบสำรองของระบบสารสนเทศและ
การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหาย ถูกทำลาย หรือถูกเปลี่ยนแปลงจากไวรัสคอมพิวเตอร์ โปรแกรมชุดคำสั่งไม่พึงประสงค์ ผู้บุกรุกทำลาย โดยสามารถนำกู้ข้อมูลที่มีปัญหากลับมาใช้งานได้

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการสำรองข้อมูลเพื่อความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

๑. ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. การพิจารณาคัดเลือกและจัดทำระบบสำรองของระบบสารสนเทศ

การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม โดยจำแนกระบบสารสนเทศตามการสนับสนุนระดับการทำงานในสถาบันเพื่อกำหนดความสำคัญของข้อมูล และความถี่ในการสำรองข้อมูล

แนวทางปฏิบัติ

๑.๑ การสำรองข้อมูล (Back up) ข้อมูลแบ่งเป็น ๒ ส่วน คือ

๑.๑.๑. ข้อมูลในส่วนของ Data แบ่งเป็น ๒ ประเภท ดังนี้

๑.๑.๑.๑ ระบบประมวลผลรายการ (Transaction Processing Systems - TPS) เป็นระบบที่ทำหน้าที่ในการปฏิบัติงานประจำทำการบันทึกจัดเก็บประมวลผลรายการที่เกิดขึ้นในแต่ละวัน โดยใช้ระบบคอมพิวเตอร์ทำงานแทนการทำงานด้วยมือ ทั้งนี้เพื่อที่จะทำการสรุปข้อมูลเพื่อสร้างเป็นสารสนเทศ ระบบประมวลผลรายการนี้ ส่วนใหญ่จะเป็นระบบที่เชื่อมโยงกิจการกับผู้รับบริการ ตัวอย่าง เช่น ระบบรายงานผลวิเคราะห์ที่ดินรายแปลง ผัก ระบบสำรวจแผนที่ เป็นต้น ในระบบต้องสร้างฐานข้อมูลที่

จำเป็น ซึ่งระบบมักจัดทำเพื่อสนองความต้องการของผู้บริหารระดับต้นเป็นส่วนใหญ่ เพื่อให้สามารถปฏิบัติงานประจำได้ ผลลัพธ์ของระบบนี้มักจะอยู่ในรูปของรายงานที่มีรายละเอียด รายงานผลเบื้องต้น ข้อมูลมีอัตราการเปลี่ยนแปลงมาก พิจารณาความถี่สูงในการสำรองข้อมูล อย่างน้อยวันละ ๒ ครั้ง สำหรับข้อมูลมีการเปลี่ยนแปลงปานกลางในการสำรองข้อมูลอย่างน้อยวันละ ๑ ครั้ง

๑.๑.๑.๒ ระบบองค์ความรู้เพื่อการพัฒนาพื้นที่สูง (Knowledge for Sustainable Highland Development – H-KM) เป็นระบบที่ช่วยสนับสนุนบุคลากรที่ทำงานด้านวิชาการ ได้รวบรวมความรู้ด้านการเกษตรและการพัฒนาพื้นที่สูง ซึ่งเป็นองค์ความรู้จากการทำงานของโครงการหลวงและขยายผลโครงการหลวง จำแนกเป็นความรู้รายสาขา ความรู้จากการวิจัยและสื่อต่างๆ เป็นข้อมูลผลงาน ผลการวิจัย ข้อมูลผัก ไม้ผลบนที่สูง การสำรวจที่ดินรายแปลง การใช้ประโยชน์ที่ดิน ข้อมูลด้านแผนที่ การสร้างความรู้เพื่อพัฒนาการคิดค้น สร้างผลิตภัณฑ์ใหม่ๆ บริการใหม่ความรู้ใหม่เพื่อนำไปใช้ประโยชน์ในสถาบัน และสถาบันควรนำเทคโนโลยีสารสนเทศเข้ามาสนับสนุนให้การพัฒนาเกิดขึ้นโดยสะดวก ผลลัพธ์ของระบบนี้ ผลการดำเนินงาน ผลงานวิจัยที่ต้องใช้ระยะเวลาในการดำเนินการจึงจะนำขึ้นเผยแพร่ผ่านระบบสารสนเทศ สำหรับข้อมูลมีอัตราการเปลี่ยนแปลงน้อยจะพิจารณาความถี่ต่ำในการสำรองข้อมูลเดือนละ ๑ ครั้ง

๑.๑.๒ ส่วนที่ ๒ ข้อมูลในส่วนของ Software หรือ Source Code

๑.๑.๒.๑ เป็นข้อมูลในส่วนของ Software หรือ Source Code เป็นชุดคำสั่งหรือโค๊ดในโปรแกรมที่พัฒนาขึ้นด้วยภาษาคอมพิวเตอร์ ภาษาต่างๆ เช่น C, java, ASP, ASP.Net, PHP เป็นต้น สำหรับข้อมูลมีการเปลี่ยนแปลงน้อยจะพิจารณาความถี่ต่ำในการสำรองข้อมูล เดือนละ ๑ ครั้ง

๑.๒ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการวัน/เวลา ชื่อข้อมูลที่สำรอง สถานการณ์สำรองข้อมูล เป็นต้น

๑.๓ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และหากพบว่าผิดปกติต้องจัดทำบันทึกและดำเนินการแก้ไขโดยทันที

๑.๔ กรณีที่จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล ต้องชี้บ่งสื่อบันทึกข้อมูลไว้อย่างชัดเจน โดยมีรายละเอียดของ ชื่อ วัน/เวลาสำรองข้อมูล ผู้รับผิดชอบ โดยสื่อสำรองข้อมูลจะต้องจัดเก็บไว้อย่างปลอดภัย และข้อมูลที่สำรองต้องเข้ารหัสเพื่อความปลอดภัย

๑.๕ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การเกิดโรคระบาดจนไม่สามารถเข้ามาปฏิบัติงานในสถานที่ทำงานได้ เป็นต้น ทั้งนี้สอดคล้องตามแผนฉุกเฉินด้านสารสเทศที่กำหนดไว้

๑.๖ วางแผนทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอเพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ และสามารถนำข้อมูลที่สำรองกลับมาใช้งานได้ (restore) โดยการทดสอบต้องจัดทำบันทึกการทดสอลไว้เป็นหลักฐาน

๑.๗ ในการกู้คืนข้อมูลศูนย์ข้อมูลและสารสนเทศ ควรดำเนินการกู้คืนข้อมูลระบบต่างๆ ของระบบสารสนเทศ สำหรับข้อมูลที่มีอัตราการเปลี่ยนแปลงมากสามารถดำเนินการกู้ข้อมูลย้อนหลัง ๑๕ วัน นับจากวันที่ข้อมูลสูญหาย และสำหรับข้อมูลที่มีอัตราการเปลี่ยนแปลงปานกลางสามารถดำเนินการกู้ข้อมูลได้ย้อนหลัง ๓๐ วัน นับจากวันที่ข้อมูลสูญหาย และสำหรับข้อมูลที่มีอัตราการเปลี่ยนแปลงน้อยสามารถดำเนินการกู้ข้อมูลได้ย้อนหลัง ๖๐ วัน นับจากวันที่ข้อมูลสูญหาย

๒. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียม ความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ โดยมีแนวทางปฏิบัติดังนี้

๒.๑ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

- ๒.๑.๑ กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
- ๒.๑.๒ ประเมินความเสี่ยงสำหรับสถานการณ์ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและทำให้เกิดการหยุดชะงักตามเกณฑ์การประเมินความเสี่ยงของ สวพส.
- ๒.๑.๓ มีการจัดทำแผนบริหารความเสี่ยงเพื่อรองรับสถานการณ์ฉุกเฉินจากการเกิดภัยพิบัติ ตาม “แผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศเมื่อเกิดเหตุการณ์ฉุกเฉิน”
- ๒.๑.๔ กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ และทดสอบการกู้คืนข้อมูลที่สำรองไว้
- ๒.๑.๕ กำหนดช่องทางในการติดต่อเมื่อเกิดกรณีฉุกเฉิน ทั้งผู้รับผิดชอบภายในสถาบันและผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อผู้ให้บริการ
- ๒.๑.๖ มีการสร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับ ใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

๒.๓ กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๒.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบ แผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง

๒.๕ ทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่ เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

๓. ระบบไฟฟ้าสำรอง

ศูนย์ข้อมูลและสารสนเทศ ดำเนินการติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) หรือแหล่งพลังงานสำรอง สำหรับให้บริการระบบเครือข่าย เครื่องแม่ข่าย และ Network เพื่อให้ยังคงใช้งานได้ในกรณีฉุกเฉิน เช่น ไฟฟ้าดับ เป็นต้น

ส่วนที่ ๓
นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(IT Risk Management)

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศขององค์กร เพื่อให้มั่นใจว่านโยบายและมาตรฐานต่างๆ ด้านความมั่นคงปลอดภัยสารสนเทศได้มีการปฏิบัติตามอย่างมีประสิทธิผล

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
๒. ผู้ตรวจสอบภายใน (Internal Audit)
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. ในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ให้ปฏิบัติดังนี้

๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจจะเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อย ๑ ครั้งต่อปี

๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. มีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

๒.๑ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๒.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อย ๑ ครั้งต่อปี

๒.๓ มีตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจสอบภายในขององค์กร (Internal Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๔ ข้อกำหนดในการดำเนินการตรวจสอบและประเมินความเสี่ยง ให้ปฏิบัติดังนี้

๒.๔๑ ให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๒.๔.๒ ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งให้มีการทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๒.๔.๓ ให้มีการระบุจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๒.๔.๔ ควรให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลประวัติแสดงการเข้าถึงนั้น (Logs) ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

๒.๔.๕ ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

๓. ข้อกำหนดการแจ้งเหตุด้านความมั่นคงปลอดภัย ให้ปฏิบัติดังนี้

๓.๑ แจ้งไปยังผู้ดูแลระบบของ สวพส. โดยทันทีเมื่อพบเหตุ

๓.๑.๑ การกระทำที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๓.๑.๒ การกระทำที่ขัดต่อความมั่นคงของชาติ

๓.๑.๓ การใช้ทรัพยากรสารสนเทศของ สวพส. ไม่เหมาะสม ผิดวัตถุประสงค์

๓.๑.๔ หน้าเว็บไซต์หลัก หรือ ระบบงานของ สวพส. ถูกเปลี่ยนแปลงโดยผู้ไม่ประสงค์ดี

๓.๑.๕ หน้าเว็บไซต์หลัก หรือ ระบบงานของ สวพส. ไม่ถูกต้อง หรือคาดเคลื่อนจากความเป็นจริง

๓.๑.๖ ข้อมูลสารสนเทศสำคัญของ สวพส. หรือส่วนตัวถูกเปิดเผย เปลี่ยนแปลง ลบ หรือ สูญหาย ก็โดยไม่ได้รับอนุญาต

๓.๑.๗ มีการนำข้อมูลสารสนเทศสำคัญของ สวพส. ไปใช้ผิดวัตถุประสงค์

๓.๑.๘ ทรัพยากรสารสนเทศถูกขโมย

๓.๑.๙ มีบุคคลภายนอกเข้าใช้งานระบบสารสนเทศของ สวพส. โดยไม่ได้รับอนุญาต

๓.๑.๑๐ มีการแอบติดตั้งอุปกรณ์ หรือโปรแกรมเพื่อดักขโมยข้อมูล หรือดักฟัง ดักดูข้อมูลในระบบเครือข่ายของ สวพส.

๓.๑.๑๑ มีการใช้อำนาจของสิทธิการเป็นผู้ดูแลระบบอย่างไม่เหมาะสม

๓.๑.๑๒ มีการบุกรุกศูนย์ข้อมูลฯ และเครือข่ายคอมพิวเตอร์ของ สวพส.

๓.๑.๑๓ มีการบุกรุกหรือการใช้โปรแกรมของผู้ไม่ประสงค์ดี

๓.๑.๑๔ เหตุการณ์อื่นๆ ที่เป็นการละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๓.๒ การจัดการกับเหตุด้านความมั่นคงปลอดภัยเมื่อได้รับรายงานเหตุด้านความมั่นคงปลอดภัย ให้ผู้ดูแลที่ได้รับมอบหมายปฏิบัติตามขั้นตอนปฏิบัติตามแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๓.๓ ให้ความร่วมมือและให้ความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลระบบที่เกี่ยวข้องในการตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น รวมถึงปฏิบัติตามคำแนะนำของผู้บังคับบัญชา และผู้ดูแลระบบที่เกี่ยวข้อง

ส่วนที่ ๔
นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้บุคลากรขององค์กร ได้รับทราบ เข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตลอดจนสามารถนาไปปฏิบัติได้อย่างถูกต้องเหมาะสม

ผู้รับผิดชอบ

๑. ศูนย์ข้อมูลและสารสนเทศ สำนักยุทธศาสตร์และแผน
๒. กลุ่มงานทรัพยากรมนุษย์ สำนักอำนวยการ
๓. หน่วยงานที่ได้รับมอบหมายในการฝึกอบรม
๔. ผู้ดูแลระบบที่ได้รับมอบหมาย
๕. เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของสถาบัน

๒. เผยแพร่ความรู้เกี่ยวกับนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย และมีการเปลี่ยนเกร็ดความรู้อยู่เสมอ ผ่านทางการติดประกาศประชาสัมพันธ์ แผ่นพับ และผ่านเว็บไซต์ของสถาบัน

๓. จัดทำคู่มือการใช้ระบบเทคโนโลยีสารสนเทศอย่างปลอดภัย และให้มีการเผยแพร่ทางหนังสือเวียนและทางเว็บไซต์ของ สวพส.

๔. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน