



## ประกาศสถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2559

เพื่อให้ข้อมูลสารสนเทศรวมทั้งระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี (สสวท.) เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยสอดคล้องตามหลักมาตรฐานสากล เชื่อถือได้ และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งเพื่อให้เกิดมาตรการในการป้องกันปัญหาอันอาจเกิดขึ้นจากภัยคุกคามต่าง ๆ และจากการใช้งานระบบเทคโนโลยีสารสนเทศ และการสื่อสารในลักษณะที่ไม่พึงประสงค์ ซึ่งอาจก่อให้เกิดความเสียหายแก่ สสวท. และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และกฎหมายอื่นที่เกี่ยวข้องได้ สสวท. จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

อาศัยอำนาจตามความในมาตรา 5 และมาตรา 7 แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 และด้วยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศไว้ดังต่อไปนี้

1. ประกาศนี้เรียกว่า “ประกาศสถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2559”
2. ประกาศนี้ให้ใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป
3. บรรดาประกาศ ระเบียบ คำสั่ง หรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน
4. นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศได้กำหนดขึ้น โดยมีวัตถุประสงค์ดังต่อไปนี้
  - 4.1 เพื่อให้มีนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศของ สสวท.
  - 4.2 เพื่อเป็นกรอบมาตรฐาน และแนวปฏิบัติในการปฏิบัติงานด้านสารสนเทศ และระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำหรับบุคลากร สสวท. และบุคคลภายนอกที่ปฏิบัติงานให้กับ สสวท.
  - 4.3 เพื่อสร้างความเข้าใจ ให้เกิดความตระหนัก และมีส่วนร่วมรับผิดชอบในการรักษาความมั่นคงปลอดภัยของสารสนเทศ

- 4.4 เพื่อเผยแพร่ให้บุคลากร สสวท. บุคคลภายนอกที่ปฏิบัติงานให้กับ สสวท. ได้รับทราบ และปฏิบัติตามอย่างเคร่งครัด
- 4.5 เพื่อติดตามการดำเนินงานและทบทวนนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับสภาพแวดล้อมและกฎหมายที่เกี่ยวข้อง อย่างน้อยปีละ 1 ครั้ง
5. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สสวท. กำหนดดังนี้
  - 5.1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ
    - 5.1.1 การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้ เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนด โดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
    - 5.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน ต้องควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ให้ผู้ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความรู้ตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศเข้าถึงระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ บริหารจัดการรหัสผ่าน ให้เข้าถึงสารสนเทศให้เหมาะสมตามลำดับชั้นความลับของผู้ใช้งาน และต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานตามระยะเวลาที่กำหนดไว้ และตรวจสอบการละเมิดความปลอดภัยเสมอ
    - 5.1.3 การควบคุมการเข้าถึงระบบเครือข่าย ต้องป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิในการเข้าถึงเครือข่ายให้ผู้ที่ จะเข้าใช้งาน ต้องลงบันทึกเข้าใช้งานเพื่อแสดงตัวตนด้วยชื่อผู้ใช้งาน ต้องมีการพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบการรักษาความปลอดภัยที่ สสวท. ได้ติดตั้งไว้ และให้จัดแบ่งระบบเครือข่ายแบบแบ่งโซน (Zone) การใช้งาน เพื่อให้การควบคุมและป้องกันภัยคุกคามให้เป็นระบบสอดคล้องกับมาตรฐานและมีประสิทธิภาพ
    - 5.1.4 การควบคุมการเข้าถึงระบบปฏิบัติการ ต้องป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ต้องกำหนดให้ผู้ที่ จะเข้าใช้งาน ต้องลงบันทึกเข้าใช้งานเพื่อแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ตัวตนด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ตลอดจนกำหนดมาตรการในการใช้งาน

โปรแกรมหรือรถยนต์ต่าง ๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

5.1.5 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ ต้องกำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชัน ต่าง ๆ รวมถึงจดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต และระบบงานต่าง ๆ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

5.1.6 การจัดทำระบบสำรองของสารสนเทศ ต้องจัดทำระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และสำรองระบบข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอ ตรวจสอบระยะเวลาในการกู้ระบบกลับคืนให้ได้ภายในระยะเวลาที่เหมาะสม และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สสวท. สามารถใช้งานได้ เป็นปกติอย่างต่อเนื่อง เหมาะสม และสอดคล้องตามภารกิจ

5.1.7 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอโดยให้มีการตรวจสอบและควบคุมประสิทธิภาพของระบบงานเทคโนโลยีสารสนเทศและการสื่อสาร และดำเนินการตรวจประเมินระบบความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สสวท. โดยผู้ตรวจสอบภายในอย่างน้อยปีละ 1 ครั้ง หรือผู้ตรวจสอบจากภายนอกอย่างน้อย 2 ปีครั้ง

5.1.8 การสร้างองค์ความรู้ และความตระหนักรู้ด้านความมั่นคงปลอดภัย กำหนดให้มีกิจกรรมอบรม จัดกิจกรรม หรือเผยแพร่สื่อด้านความมั่นคงปลอดภัย เพื่อให้ความรู้สร้างความเข้าใจแก่ผู้ใช้งานในสาระสำคัญที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของสารสนเทศ และตระหนักถึงภัยและผลกระทบที่อาจเกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมทั้งส่งเสริมการพัฒนาบุคลากรที่เกี่ยวข้องให้มีความสามารถในการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยต่างๆ และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่คาดคิดได้

6. การกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสาร ของทางราชการ พ.ศ.2540 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 หรือข้อกำหนดอื่นที่ได้ประกาศใช้ทดแทน

7. กำหนดให้ผู้บริหารระดับสูง ซึ่งเป็นผู้กำกับดูแลสำนักเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบในการกำกับดูแลให้เป็นไปตามประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
8. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเสียหาย หรืออันตรายใด ๆ แก่ สสวท.หรือ ผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงสุด เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น
9. สสวท.ต้องจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และกำหนดให้บุคลากร สสวท.และ บุคคลภายนอกที่ปฏิบัติงานให้กับ สสวท. ปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศดังกล่าวอย่างเคร่งครัด

ประกาศ ณ วันที่ 3 สิงหาคม พ.ศ. 2559

  
(นางพรพรรณ เวทยางกูร)

ผู้อำนวยการสถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี

ใช้สำหรับการประชุมจัดทำนโยบาย แผนปฏิบัติการ PDPA สสวท. เท่านั้น



## ประกาศสถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี

### เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2559

เพื่อให้เป็นไปตามนโยบายการรักษาความมั่นคงปลอดภัยในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี เห็นสมควรให้มีการกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ไว้ดังต่อไปนี้

#### คำนิยาม

1. **หน่วยงาน** หมายความว่า สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี
2. **ฝ่าย** หมายความว่า ฝ่ายเทคโนโลยีสารสนเทศ
3. **ผู้ใช้งาน** หมายความว่า พนักงาน พนักงานสมทบ ลูกจ้างตามสัญญาจ้าง ในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน
4. **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
5. **สินทรัพย์** หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับหน่วยงาน
6. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบสารสนเทศหรือระบบเครือข่าย ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ
7. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายความว่า การดำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งาน ของระบบเทคโนโลยีสารสนเทศ รวมทั้งคุณสมบัติอื่นๆ ได้แก่ ความถูกต้องแท้จริง ความรับผิดชอบ การห้ามปฏิเสธความรับผิดชอบ และความน่าเชื่อถือ

8. เหตุการณ์ด้านความมั่นคงปลอดภัย หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
9. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
10. ระบบอินเทอร์เน็ต (internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อ ระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล
11. ระบบสารสนเทศ หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการ วางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น
12. ระบบเครือข่าย หมายถึง กลุ่มของคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่ถูกนำมาเชื่อมต่อกันเพื่อให้ผู้ใช้งานในระบบเครือข่ายสามารถติดต่อสื่อสารแลกเปลี่ยน เปลี่ยนข้อมูล และใช้อุปกรณ์ในระบบเครือข่าย ในระบบเครือข่ายร่วมกันได้
13. อุปกรณ์ในระบบเครือข่าย หมายถึง อุปกรณ์ที่ใช้สำหรับบริหารจัดการ ควบคุมความปลอดภัยของการทำงานได้แก่ Router Firewall Switch SSL VPN เป็นต้น
14. ผู้ดูแลระบบ หมายความว่า ผู้ดูแลระบบสารสนเทศ (System Administrator) และ/หรือ ผู้ดูแลระบบเครือข่าย (Network Administrator)
15. ผู้ดูแลระบบสารสนเทศ (System Administrator) หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์ ได้แก่ ระบบจดหมายอิเล็กทรอนิกส์ ระบบฐานข้อมูลในแต่ละระบบ Web Server ระบบ SharePoint
16. ผู้ดูแลระบบเครือข่าย (Network Administrator) หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด
17. หน่วยงานภายนอก หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการทำงานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจ หน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

18. **จดหมายอิเล็กทรอนิกส์ (e-Mail)** หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP POP3 และ IMAP
19. **สื่อบันทึกพกพา** หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ flash drive หรือ handy drive หรือ thumb drive หรือ external hard disk หรือ floppy disk เป็นต้น
20. **ชื่อผู้ใช้ (user name)** หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้
21. **รหัสผ่าน (password)** หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือ ในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคง ปลอดภัย ของข้อมูลและระบบเทคโนโลยีสารสนเทศ
22. **การเข้ารหัส (encryption)** หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ ตามปกติ
23. **การพิสูจน์ยืนยันตัวตน (authentication)** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการ เข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ ชื่อผู้ใช้ (user name) และรหัสผ่าน (password)
24. **SSID (Service Set Identifier)** หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่าย ที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน
25. **WEP (Wired Equivalent Privacy)** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัย ของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่ รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้
26. **WPA (Wi-Fi Protected Access)** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของ ข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)
27. **MAC Address (Media Access Control Address)** หมายความว่า หมายเลขเฉพาะที่ใช้อ้างอิง ถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ดโดยแต่ละการ์ดจะมีหลายเลขที่ ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน 16 จำนวน 6 คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการ ส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

28. แผนผังระบบเครือข่าย (Network Diagram) หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน
29. SSL VPN (Secure Sockets Layer Virtual Private Network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

ใช้สำหรับการประชุมจัดทำนโยบาย แนวปฏิบัติ PDPA สลาวท. เท่านั้น



## เอกสารหมวดที่ 1

### การควบคุมการเข้าถึงระบบสารสนเทศ

ส่วน	เรื่อง	หน้า
ส่วนที่ 1	การควบคุมการเข้าถึงสารสนเทศ	6
ส่วนที่ 2	การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)	9
ส่วนที่ 3	หน้าที่รับผิดชอบของผู้ใช้งาน (User Responsibilities)	12
ส่วนที่ 4	การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)	14
ส่วนที่ 5	การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	17
ส่วนที่ 6	การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)	20
ส่วนที่ 7	การควบคุมการเข้าถึงเครื่องแม่ข่าย (Server)	23
ส่วนที่ 8	ความมั่นคงปลอดภัยด้านกายภาพ (Physical Security)	24

## หมวดที่ 1

### การควบคุมการเข้าถึงระบบสารสนเทศ

#### วัตถุประสงค์

1. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ และการมอบอำนาจของหน่วยงานในสังกัด สสวท.
2. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
3. เพื่อให้ผู้รับผิดชอบและผู้ที่เกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้แก่ สสวท. ได้รับรู้ เข้าใจ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย และสามารถยึดถือไปปฏิบัติตามข้อกำหนดในแนวทางที่กำหนดไว้ได้อย่างเคร่งครัด

#### ผู้รับผิดชอบ

1. ฝ่ายเทคโนโลยีสารสนเทศ
2. ผู้ใช้งาน

#### ขอบเขต

แนวปฏิบัติในหมวดนี้ครอบคลุมถึง พนักงาน ลูกจ้าง และ บุคคลภายนอกที่มีการดำเนินการเกี่ยวกับระบบสารสนเทศของ สสวท.

## ส่วนที่ 1

### การควบคุมการเข้าถึงสารสนเทศ

เพื่อควบคุมการเข้าถึงระบบสารสนเทศโดยให้เข้าถึงสารสนเทศได้เฉพาะผู้ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

#### 1. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงและใช้งานระบบสารสนเทศ ดังนี้

- 1) ผู้เป็นเจ้าของระบบงาน เจ้าของข้อมูล หรือผู้ที่ได้รับมอบหมายเท่านั้นทำหน้าที่เป็นผู้อนุมัติการเข้าถึงระบบงาน เฉพาะส่วนที่จำเป็นต่อการใช้งานตามหน้าที่ หรือควมเหมาะสมเท่านั้น
- 2) การกำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้องให้กำหนดดังนี้ อย่างน้อยๆ สร้างข้อมูล ป้อนข้อมูล แก้ไข อนุมัติ ไม่มีสิทธิ
- 3) ผู้ดูแลระบบ รับมอบสิทธิในการกำหนดการอนุญาต สิทธิในการเข้าถึงสารสนเทศให้ผู้ใช้งานเข้าถึงระบบสารสนเทศตามข้อกำหนดของผู้เป็นเจ้าของระบบงาน เจ้าของข้อมูล หรือผู้ที่ได้รับมอบหมายเท่านั้น
- 4) ผู้ดูแลระบบสารสนเทศมีหน้าที่ทบทวน ตรวจสอบการอนุญาต สิทธิร่วมกับเจ้าของระบบงาน เจ้าของข้อมูล หรือผู้ที่ได้รับมอบหมาย อย่างสม่ำเสมอ
- 5) กรณีผู้ใช้งานจำเป็นต้องการใช้งานระบบสารสนเทศในส่วนที่นอกเหนือจากหน้าที่ความรับผิดชอบของตนเอง จะต้องได้รับอนุญาตจากหัวหน้าหน่วยงานกำกับดูแล และหัวหน้าหน่วยงานผู้กำกับดูแลผู้เป็นเจ้าของระบบงาน เจ้าของข้อมูล หรือผู้ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร
- 6) บุคคลจากหน่วยงานภายนอก สสวท. ที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของหน่วยงานภายใน สสวท. จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อหัวหน้าหน่วยงาน
- 7) กำหนดเกณฑ์ระดับสิทธิมอบอำนาจ ให้เป็นไปตามการบริหารโดยให้ดำเนินการตามที่กำหนดไว้ในส่วนที่ 2 การบริหารจัดการการเข้าถึงของผู้ใช้งานว่าด้วยการบริหารสิทธิของผู้ใช้งานในการใช้งานระบบ (Privilege Management)

## 2. ข้อกำหนดด้านข้อมูลสารสนเทศ

1) ข้อมูลสารสนเทศของ สสวท. สามารถแบ่งได้เป็น 3 ประเภทดังนี้

- ข้อมูลสารสนเทศสำหรับการบริหารงาน ได้แก่ ข้อมูลบุคลากร ข้อมูลงบประมาณ ข้อมูลการเงิน – การบัญชี
- ข้อมูลสารสนเทศด้านการบริการพนักงานของ สสวท. ได้แก่ ระบบสารสนเทศสำหรับพนักงาน (MIS) ระบบจดหมายอิเล็กทรอนิกส์ ระบบบริหารจัดการเอกสาร ระบบจัดเก็บเอกสาร
- ข้อมูลสารสนเทศด้านการบริการ ครู นักเรียน และบุคคลทั่วไป ได้แก่ ข้อมูลประชาสัมพันธ์ ข่าวตัด/ข่าวแจก ข้อมูลที่เผยแพร่ผ่านทางเว็บไซต์และสื่อสังคมออนไลน์ของ สสวท.

2) ระดับความลับของข้อมูลสารสนเทศสามารถแบ่งออกเป็น 3 ระดับ ตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.2540 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ดังต่อไปนี้

- ข้อมูลลับที่สุด (Top Secret) กล่าวคือ หากข้อมูลเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายร้ายแรงที่สุด ได้แก่ ข้อมูลที่ผู้อำนวยการ สสวท. กำหนดให้มีความสำคัญในระดับลับที่สุด
- ข้อมูลลับมาก (Secret) กล่าวคือ หากข้อมูลเปิดเผยทั้งหมดหรือเพียงบางส่วน ก่อให้เกิดความเสียหายร้ายแรง ได้แก่ ข้อมูลสารสนเทศ ผู้อำนวยการฝ่าย/สาขา/โครงการ ผู้ช่วยผู้อำนวยการ รองผู้อำนวยการ ให้มีความสำคัญในระดับลับมาก
- ข้อมูลลับ (Confidential) กล่าวคือ หากข้อมูลเปิดเผยทั้งหมดหรือเพียงบางส่วน ก่อให้เกิดความเสียหายโดย ผู้อำนวยการส่วน หรือหัวหน้างานให้มีความสำคัญในระดับลับ

3) การกำหนดระดับชั้นการเข้าถึง แบ่งออกเป็น 3 ระดับได้ ดังนี้

- เข้าถึงได้ทุกผู้ใช้งาน: ข้อมูลที่มีระดับชั้นการเข้าถึงนี้ ได้แก่ ข้อมูลสารสนเทศเพื่อการบริการ
- เข้าถึงได้เฉพาะผู้ใช้งานที่ได้รับสิทธิ: ข้อมูลที่มีระดับชั้นการเข้าถึงนี้ ได้แก่ ข้อมูลสารสนเทศบริการพนักงาน

- เข้าถึงได้เฉพาะผู้บริหาร โดยแบ่งชั้นการเข้าถึงได้ดังนี้
  - ข้อมูลลับที่สุด (Top Secret) เข้าถึงได้เฉพาะ ผู้อำนวยการ สสวท. หรือผู้ที่ผู้อำนวยการ สสวท. มอบหมาย
  - ข้อมูลลับมาก (Secret) เข้าถึงได้เฉพาะ ผู้อำนวยการฝ่าย/สาขา/โครงการ ผู้ช่วยผู้อำนวยการ รองผู้อำนวยการ หรือ ผู้ที่ผู้อำนวยการ สสวท. มอบหมาย
  - ข้อมูลลับ (Confidential) เข้าถึงได้เฉพาะ ผู้อำนวยการส่วน หรือหัวหน้างานผู้บริหารระบบเครือข่าย/ระบบสารสนเทศ หรือผู้ที่ผู้อำนวยการ สสวท. มอบหมาย

4) การรักษาความลับของข้อมูล

- ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 เว้นแต่จะประกาศไว้เป็นอย่างอื่น
- การรับส่งข้อมูลที่เป็นความลับผ่านระบบเครือข่ายสาธารณะต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากล

5) ช่องทางและช่วงเวลาการเข้าถึงข้อมูล

- ผู้ใช้งานสามารถเข้าใช้บริการระบบสารสนเทศได้ผ่านทางระบบเครือข่ายภายในของ สสวท. ได้ตลอด 24 ชั่วโมง
- ผู้ใช้งานสามารถเข้าใช้งานระบบสารสนเทศจากระบบอินเทอร์เน็ต เมื่ออยู่ภายนอก สสวท. ได้ทาง SSL VPN ได้ตลอด 24 ชั่วโมง

## ส่วนที่ 2

### การบริหารจัดการการเข้าถึงของผู้ใช้งาน

#### (User Access Management)

##### 1. การลงทะเบียนผู้ใช้งาน (User Registration)

กำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานใหม่เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น/ตามภาระงานเท่านั้น

- 1) ฝ่ายทรัพยากรบุคคลและพัฒนองค์กรหรือหน่วยงานต้นสังกัด แจ้งข้อมูลของลงทะเบียนผู้ใช้งานใหม่  
มายังผู้ดูแลระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร
- 2) ผู้ดูแลระบบสารสนเทศตรวจสอบข้อมูลผู้ลงทะเบียนใหม่
- 3) ผู้ดูแลระบบสารสนเทศพิจารณาอนุมัติให้ลงทะเบียนผู้ใช้งานใหม่ และแจ้งผลการอนุมัติกลับไปยังฝ่ายทรัพยากรบุคคลและพัฒนองค์กรหรือหน่วยงานต้นสังกัด และผู้ใช้งานใหม่ให้ทราบต่อไป
- 4) ผู้ดูแลระบบต้องจัดเก็บข้อมูลของการลงทะเบียนผู้ใช้งานใหม่ที่ขอเข้าใช้งานระบบสารสนเทศเพื่อเอาไว้ใช้อ้างอิงหรือตรวจสอบภายหลัง

##### 2. การบริหารสิทธิของผู้ใช้งานในการใช้งานระบบ (Privilege Management)

ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงดังนี้

- 1) ผู้ดูแลระบบสารสนเทศอนุญาตให้ผู้ใช้งานมีสิทธิในการเข้าถึงระบบสารสนเทศได้ดังต่อไปนี้
  - พนักงานของ สสวท. ทุกคนจะมีสิทธิในการใช้งานระบบดังต่อไปนี้ ได้แก่
    - ระบบ Internet
    - ระบบ Wi-Fi (IPST-Staff)
    - ระบบ Intranet
    - ระบบ e-Mail
    - ระบบ SSL VPN
    - ระบบบริการพนักงาน
  - กลุ่มผู้บริหาร ได้แก่ ผู้อำนวยการ สสวท. รองผู้อำนวยการ ผู้ช่วยผู้อำนวยการ ผู้อำนวยการฝ่าย/สาขา/โครงการ จะได้รับสิทธิเพิ่มเติมจากสิทธิของพนักงาน สสวท. ในการเข้าถึงระบบสารสนเทศดังนี้
    - ระบบ Business Intelligence (BI)

- กลุ่มผู้ดูแลระบบจะได้รับสิทธิเพิ่มเติมจากสิทธิของพนักงาน สสวท. ในการเข้าถึงระบบสารสนเทศดังนี้
    - ระบบบริหารจัดการ Account
    - ระบบบริหารจัดการ e-Mail
    - ระบบบริหารจัดการ Network
    - ระบบบริหารจัดการ Server
    - ระบบบริหารจัดการ MIS
  - สำหรับบุคคลภายนอกจะมีสิทธิในการเข้าถึงระบบดังนี้
    - ระบบ Internet
    - ระบบ Wi-Fi (IPST-Guest)
- 2) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานใช้ระบบสารสนเทศได้ตามที่ได้รับอนุญาตเท่านั้น
  - 3) ในกรณีมีความจำเป็นที่ต้องให้ผู้ใช้งานมีสิทธิพิเศษมากกว่าที่กำหนดไว้ข้างต้น ต้องมีการบริหารจัดการที่รัดกุมดังต่อไปนี้
    - สิทธิในระดับ System และ สิทธิพิเศษอื่นๆ ให้กำหนด User Account หรือ User ID เฉพาะโดยไม่ปะปนกับ User Account หรือ User ID ทั่วไปของบุคลากร
    - ผู้ใช้งานผู้นั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา
    - มีการกำหนดระยะเวลาการใช้งานและต้องระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง
  - 4) ผู้ดูแลระบบสารสนเทศกำหนดบัญชีผู้เข้าใช้งาน (Account) แยกกันเป็นรายบุคคล กล่าวคือไม่กำหนดบัญชีผู้เข้าใช้งานซ้ำซ้อนกัน และถือว่าบัญชีผู้ใช้งานเป็นการระบุและยืนยันตัวตนของผู้ใช้งานต่อไป
  - 5) ผู้ดูแลระบบสารสนเทศจำกัดการใช้งานบัญชีชื่อผู้ใช้งานแบบกลุ่มซึ่งมีการใช้งานร่วมกัน กล่าวคืออนุญาตให้ใช้งานได้ก็ต่อเมื่อมีเหตุผลความจำเป็นในการใช้งานเท่านั้นและบัญชีผู้ใช้งานแบบกลุ่มต้องรับผิดชอบการใช้งานร่วมกัน
  - 6) ผู้ดูแลระบบต้องไม่อนุญาตให้ผู้ร้องขอใช้ระบบงานสารสนเทศเข้าใช้ระบบจนกว่าจะได้รับอนุมัติแล้วเท่านั้น
  - 7) ผู้ใช้งานต้องลงนามรับทราบสิทธิและหน้าที่ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

### 3. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

- 1) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตนโดยลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศของหน่วยงาน
- 2) การมอบรหัสผ่านให้แก่ผู้ใช้งานในครั้งแรก ให้กำหนดรหัสผ่านชั่วคราวโดยวิธีการสุ่มให้กับผู้ใช้งาน เมื่อผู้ใช้งานได้รับรหัสผ่านแล้ว ให้เปลี่ยนรหัสผ่านนั้นเป็นรหัสผ่านของตนเองโดยตั้งรหัสผ่านตามแนวปฏิบัติการใช้/ตั้งรหัสผ่านที่ดี
- 3) การส่งมอบรหัสผ่านให้แก่ผู้ใช้งานต้องเป็นไปอย่างปลอดภัยโดยกำหนดให้ใช้วิธีการใส่ซองปิดผนึก จากนั้นจึงจะส่งมอบให้แก่ผู้ใช้งานโดยตรง
- 4) ผู้ใช้งานต้องตอบยืนยันการได้รับรหัสผ่าน
- 5) กำหนดให้หน่วยงานต้นสังกัด แจ้งผู้ดูแลระบบสารสนเทศทันที เมื่อมีผู้ใช้งานโต้บังคับบัญชาลาออก หรือไม่มีหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิใช้งาน เพื่อเปลี่ยนสิทธิหรือถอดถอนสิทธิของผู้ใช้งานออกจากระบบสารสนเทศทันทีที่ได้รับแจ้ง
- 6) ผู้ดูแลระบบสารสนเทศจัดทำระบบที่เอื้อให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านของตนเองได้ โดยกำหนดให้เปลี่ยนทุก 180 วัน
- 7) ผู้ดูแลระบบสารสนเทศต้องกำหนดจำนวนครั้งที่ยินยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดได้ไม่เกิน 5 ครั้ง

### 4. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

- 1) ผู้ดูแลระบบสารสนเทศทบทวนสิทธิการเข้าถึงของผู้ใช้งานทุกๆ 1 ปี หรือเมื่อเกิดการเปลี่ยนแปลงสิทธิของผู้ใช้งาน ได้แก่ การลาออก การย้ายแผนก/สาขา จะต้องมีการทบทวนสิทธิการใช้งานทุกครั้งอีกด้วย และต้องคืนสินทรัพย์ของ สสวท. ที่เกี่ยวข้องกับปฏิบัติงานของตนด้วย
- 2) พิมพ์รายชื่อผู้ใช้งานที่ยังมีสิทธิการใช้งานระบบสารสนเทศแยกตามหน่วยงาน
- 3) ส่งรายชื่อที่แนบมาให้กับผู้บังคับบัญชาของแต่ละฝ่ายของ สสวท. เพื่อดำเนินการทบทวนว่ามีรายชื่อที่ออกสิทธิเข้าถึงระบบสารสนเทศไปแล้วหรือมีการเปลี่ยนแปลงแต่ยังไม่ได้มีการแก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่
- 4) ผู้บังคับบัญชาของแต่ละฝ่ายของ สสวท. แจ้งหรืออนุมัติรายชื่อของผู้มีสิทธิในระบบงานสารสนเทศที่ได้รับการแก้ไขถูกต้องแล้ว
- 5) ผู้ดูแลระบบสารสนเทศดำเนินการแก้ไขข้อมูลผู้มีสิทธิให้ถูกต้องตามที่แจ้งหรือได้รับการอนุมัติ



### ส่วนที่ 3

#### หน้าที่รับผิดชอบของผู้ใช้งาน

#### (User Responsibilities)

##### 1. การใช้งานรหัสผ่านอย่างปลอดภัย

- 1) ผู้ใช้งานต้องใช้รหัสผ่านของตนเองหรือตามที่ได้รับอนุมัติเท่านั้น
- 2) ผู้ใช้งานต้องเก็บรักษารหัสผ่านที่ได้รับให้เป็นความลับ ห้ามใช้รหัสผ่านร่วมกับผู้อื่น รวมทั้งต้องไม่จดหรือบันทึกรหัสผ่านของตนไว้ในสถานที่ที่ง่ายแก่การมองเห็น
- 3) ผู้ใช้งานต้องกำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยต้องมีการผสมผสานกันระหว่าง ตัวอักษรที่เป็น ตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และตัวอักขระพิเศษเข้าด้วยกัน
- 4) ผู้ใช้งานต้องไม่กำหนดรหัสผ่านที่ง่ายแก่การคาดเดา ได้แก่ ชื่อ สกุล วันเกิด ชื่อโรงเรียน
- 5) ผู้ใช้งานต้องไม่ใช่โปรแกรมคอมพิวเตอร์ช่วยในการจดจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Remember Password Autocomplete)
- 6) กรณีผู้ใช้งานมีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นไม่ว่ากรณีใด ๆ ก็ตามเพื่อการปฏิบัติงาน หลังจากดำเนินการเรียบร้อยแล้วให้เปลี่ยนรหัสผ่านทันที
- 7) กรณีต้องการยกเลิกหรือขอรหัสผ่านใหม่ให้แจ้งเป็นลายลักษณ์อักษรมายังผู้ดูแลระบบสารสนเทศ
- 8) กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านทุก 180 วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน
- 9) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนการใช้งานระบบสารสนเทศของ สสวท. หากการพิสูจน์ตัวตนนั้นมีปัญหา ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบสารสนเทศรับทราบทันที
- 10) เมื่อผู้ใช้งานไม่อยู่ที่อุปกรณ์คอมพิวเตอร์ต้องทำการล็อกหน้าจอ/ออกจากระบบ (Logout) ทุกครั้ง และทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

##### 2. การป้องกันอุปกรณ์ขณะที่ไม่มีผู้ใช้งานที่ตัวอุปกรณ์

- 1) ผู้ใช้งานออกจากระบบสารสนเทศทันทีเสร็จสิ้นการใช้งาน
- 2) ผู้ใช้งานต้องล็อกอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว
- 3) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้อุปกรณ์คอมพิวเตอร์หรือระบบสารสนเทศของตนเอง โดยใส่รหัสผ่านให้ถูกต้องก่อนใช้งานอุปกรณ์คอมพิวเตอร์

- 4) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้อุปกรณ์คอมพิวเตอร์ทุกเครื่องทำการตั้งเวลาพักหน้าจอ (Screen Saver) โดยตั้งเวลาอย่างน้อย 15 นาที และมีการใช้รหัสผ่านในการเข้าถึงใหม่ทุกครั้ง

### 3. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

- 1) ผู้ดูแลระบบสารสนเทศจัดทำบัญชีสินทรัพย์สารสนเทศ โดยระบุผู้รับผิดชอบในสินทรัพย์สารสนเทศนั้นอย่างชัดเจน
- 2) เมื่อผู้ใช้งานมีการใช้งานสินทรัพย์ ต้องลงบันทึกการใช้งานที่ผู้ดูแลระบบจัดทำขึ้น เพื่อป้องกันการสูญหายของสินทรัพย์
- 3) ผู้ใช้งานต้องไม่ทิ้งหรือปล่อยให้สินทรัพย์ที่มีความสำคัญ ได้แก่ เอกสาร สื่อบันทึกข้อมูล อยู่ในสถานที่ที่ไม่ปลอดภัย ที่สาธารณะ หรือถูกพบเห็นได้ง่าย
- 4) ผู้ใช้งานต้องเก็บสินทรัพย์ที่ตนใช้งานในที่ที่กำหนดไว้หลังใช้งานเสร็จเรียบร้อยเรียบร้อยแล้ว หากเป็นการใช้งานระบบสารสนเทศต้องทำการออกจากระบบทุกครั้ง
- 5) ในกรณีที่มีสินทรัพย์อยู่ในรูปแบบอิเล็กทรอนิกส์และสารสนเทศนั้นถูกระบุชั้นความลับ หากมีการส่งสารสนเทศนั้นผ่านระบบ e-Mail ต้องเปิดฟังก์ชันการห้ามส่งต่อ e-Mail นั้น

### 4. การทำลายสื่อข้อมูลอิเล็กทรอนิกส์

- 1) ผู้รับผิดชอบข้อมูลอิเล็กทรอนิกส์เป็นผู้ทำลายข้อมูล
- 2) กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลายแบบนำสื่อบันทึกกลับมาใช้ใหม่ได้	ระยะเวลาการทำลาย	วิธีการทำลายแบบนำสื่อบันทึกกลับมาใช้ใหม่ไม่ได้	ระยะเวลาการทำลาย
CD/DVD	ไม่มี	ทำลายก่อนนำมาใช้ใหม่	วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย	เก็บรักษาอย่างน้อย 1 ปี หรือตามที่กฎหมายกำหนด
Flash Drive	ใช้วิธีการ Format			
เทปบันทึกข้อมูล				
Hard Drive	ใช้วิธีการ Format ตามมาตรฐานการทำลายข้อมูลบน Hard disk ของกระทรวงกลาโหมสหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็น จำนวนหลายรอบ)			

ตารางที่ 1 : วิธีการทำลายข้อมูลอิเล็กทรอนิกส์

## ส่วนที่ 4

### การควบคุมการเข้าถึงระบบเครือข่าย

#### (Network Access Control)

##### 1. การใช้งานระบบเครือข่าย

- 1) ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบเครือข่าย ให้สามารถเข้าถึงระบบเครือข่ายและระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตเท่านั้น
- 2) ผู้ดูแลระบบเครือข่ายมีหน้าที่ตรวจสอบการอนุมัติและกำหนดการอนุญาตในการผ่านเข้าสู่ระบบเครือข่าย ตามสิทธิและความจำเป็นในการปฏิบัติงานเท่านั้น
- 3) ผู้ดูแลระบบเครือข่ายจะต้องจัดให้มีการบันทึกการใช้งานของผู้ใช้งาน ตลอดจนเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัยและสิทธิการใช้งานของผู้ใช้คนอื่นๆ
- 4) การใช้งานอินเทอร์เน็ตจะถูกระงับการใช้งานไว้เป็นเวลา 90 วัน ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

##### 2. การแบ่งแยกระบบเครือข่าย (Segregation in Networks)

- 1) ผู้ดูแลระบบเครือข่ายต้องออกแบบระบบเครือข่ายโดยต้องทำการแบ่งแยกระบบเครือข่ายตามกลุ่มของระบบสารสนเทศที่มีการใช้งาน ตามกลุ่มของผู้ใช้งาน และกลุ่มระบบสารสนเทศ โดยต้องแบ่งออกเป็นเขตภายใน (Internal Zone) และเขตภายนอก (External Zone) และเขตสำหรับการให้บริการ (Demilitarized Zone: DMZ) เพื่อเป็นการควบคุมและป้องกันการถูกบุกรุกได้อย่างเป็นระบบ
- 2) ผู้ดูแลระบบสารสนเทศต้องติดตั้งเครื่องแม่ข่ายไว้ในระบบเครือข่ายที่แยกต่างหากจากระบบเครือข่ายผู้ใช้งาน และใช้ Firewall หรืออุปกรณ์เครือข่ายอื่นๆ เพื่อจำกัดให้เฉพาะกลุ่มผู้ใช้งานที่ได้รับอนุญาตเท่านั้น
- 3) สำหรับวิธีการแบ่งแยกระบบเครือข่ายนั้น สามารถทำได้ด้วยวิธีการทางกายภาพ (Physical) หรือ วิธีการแบ่งเครือข่ายออกเป็น Virtual LAN (VLAN)

##### 3. การควบคุมเส้นทางบนระบบเครือข่าย (Network Routing Control)

- 1) ผู้ดูแลระบบเครือข่ายต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย (Network Routing Table) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณข้อมูล (Switch Layer 3) เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

- 2) ผู้ดูแลระบบเครือข่ายต้องจำกัดการใช้เส้นทางบนระบบเครือข่ายจากอุปกรณ์คอมพิวเตอร์ของผู้ใช้งานไปยังเครื่องแม่ข่ายที่ให้บริการต่างๆ (Server) โดยกำหนดให้ใช้เส้นทางที่ต้องผ่าน DMZ (Demilitarize Zone)
- 3) ผู้ดูแลระบบเครือข่ายต้องจำกัดการใช้เส้นทางบนระบบเครือข่ายจากอุปกรณ์คอมพิวเตอร์ของผู้ใช้งานไปยังเครื่องแม่ข่ายที่ให้บริการต่างๆ (Server) โดยเชื่อมต่อเข้าสู่เครื่องแม่ข่ายที่ให้บริการ เพื่อบริหารจัดการระบบ ให้กำหนดเฉพาะชุด IP Address ของผู้ดูแลระบบสารสนเทศเท่านั้นที่จะสามารถเข้าถึงเครื่องแม่ข่ายให้บริการนั้นได้
- 4) ผู้ดูแลระบบเครือข่ายต้องกำหนดให้มีอุปกรณ์ Firewall เพื่อควบคุมเส้นทางบนระบบเครือข่าย

#### 4. การควบคุมการเชื่อมต่อทางระบบเครือข่าย (Network Connection Control)

- 1) ใช้ Monitoring tools เพื่อการตรวจสอบการเชื่อมต่อทางระบบเครือข่าย
- 2) มีระบบตรวจจับผู้บุกรุกทั้งในระดับระบบเครือข่าย และระดับเครื่องแม่ข่าย
- 3) มีการควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่าย โดยไม่ได้รับอนุญาต

#### 5. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก

- 1) การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username)
- 2) การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password)
- 3) การเข้าสู่ระบบสารสนเทศของ สสวท. จากอินเทอร์เน็ตนั้น จะมีการตรวจสอบผู้ใช้งานอีกครั้ง
- 4) การเข้าสู่ระบบจากระยะไกล (Remote Access) เพื่อเพิ่มความปลอดภัย จะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานและต้องมีการใช้งาน Protocol ที่มีการเข้ารหัสข้อมูล ได้แก่ SSL

#### 6. การบริหารจัดการระบบเครือข่ายสำหรับผู้ดูแลระบบเครือข่าย

- 1) กำหนดค่าเริ่มต้นพื้นฐานของทุกระบบเครือข่ายต้องเป็นแบบอนุญาตบางส่วนและปฏิเสธทั้งหมด (Permit Any & Deny All)
- 2) การเข้าถึงอุปกรณ์ระบบเครือข่ายเพื่อการตรวจสอบและปรับแต่งระบบ ต้องทำได้เพียงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น และต้องทำการสำรองข้อมูลการกำหนดค่า Configuration ทุกครั้งที่มีการเปลี่ยนแปลง พร้อมทั้งต้องบันทึกรายละเอียดของผู้ที่เข้ามาตรวจสอบและปรับแต่งระบบด้วย

- 3) มีการตรวจสอบและปิด Port ของอุปกรณ์เครือข่ายที่ไม่ได้ใช้งาน สำหรับ Port ที่ใช้ในการตรวจสอบและปรับแต่งระบบ ต้องมีการพิสูจน์ยืนยันตัวบุคคลและอนุญาตเฉพาะผู้ที่มีสิทธิเท่านั้น
- 4) กำหนดหมายเลข IP Address ให้กับอุปกรณ์เครือข่ายใดๆ ที่เชื่อมต่ออยู่กับระบบเครือข่าย เพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายได้ ให้ใช้ หมายเลข MAC Address ในการระบุถึงอุปกรณ์เครือข่ายแทน
- 5) ข้อมูลหมายเลข IP Address ของคอมพิวเตอร์ภายใน (Local) ของระบบเครือข่ายภายในของ สสวท. จำเป็นต้องมีการป้องกันไม่ให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้
- 6) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและระบบเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- 7) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่า 90 วัน

#### 7. การใช้งานระบบเครือข่ายไร้สาย (Wireless LAN)

- 1) ผู้ดูแลระบบเครือข่ายต้องกำหนดให้มีการพิสูจน์ตัวตนของผู้ใช้งานก่อนเข้าเครือข่ายไร้สาย
- 2) ผู้ดูแลระบบเครือข่ายต้องกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายกับระบบเครือข่าย รวมทั้งทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ
- 3) ผู้ดูแลระบบต้องติดตั้งอุปกรณ์ป้องกัน ได้แก่ Firewall เป็นต้น ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายใน สสวท.
- 4) ผู้ดูแลระบบเครือข่ายต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ เพื่อป้องกันไม่ให้สัญญาณรั่วไหลออกนอกพื้นที่การใช้งานเครือข่ายไร้สาย

## ส่วนที่ 5

### การควบคุมการเข้าถึงระบบปฏิบัติการ

#### (Operating System Access Control)

#### 1. การกำหนดขั้นตอนการปฏิบัติเพื่อการใช้งานระบบปฏิบัติการ

- 1) ผู้ดูแลระบบสารสนเทศกำหนดการใช้นามผู้ใช้ (Username) และรหัสผ่าน (Password) ก่อนการใช้งานระบบปฏิบัติการ
- 2) ผู้ดูแลระบบสารสนเทศตั้งค่าโปรแกรม Screen Saver เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งานเป็นเวลา 15 นาที หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้บริการจะต้องใส่รหัสผ่านเพื่อเข้าใช้งาน
- 3) ผู้ต้องใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้นามผู้ใช้และรหัสผ่านของตนในการเข้าใช้งานอุปกรณ์คอมพิวเตอร์ของ สสวท. ร่วมกัน
- 4) ผู้ใช้งานต้องทำการบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
- 5) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

#### 2. การระบุและยืนยันตัวตนของผู้เข้าใช้งาน (User Identification and Authentication)

- 1) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบสารสนเทศ โดยใช้ Username และ Password ของตนเอง เพื่อป้องกันผู้ไม่มีสิทธิในการใช้งานระบบสารสนเทศ หากการระบุและยืนยันตัวตนของผู้มีปัญหาหรือเกิดข้อผิดพลาด ให้ผู้ใช้งานแจ้งผู้ดูแลระบบสารสนเทศ ดำเนินการแก้ไข
- 2) ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้นามผู้ใช้บริการ (Account) ของอุปกรณ์คอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะสามารถพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น
- 3) ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่นๆ ห้ามโอน จำหน่าย หรือแจกจ่ายให้ผู้อื่นโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา
- 4) ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้นามผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

### 3. การบริหารจัดการรหัสผ่าน (Password Management System)

- 1) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตนเองโดยลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบสารสนเทศของหน่วยงาน
- 2) การมอบบัญชีผู้ใช้งาน (Account) ให้กับผู้ใช้งานให้ตั้งรหัสผ่านชั่วคราวด้วยวิธีการสุ่มให้กับผู้ใช้งาน
- 3) การมอบรหัสผ่านให้ผู้ใช้งานต้องเป็นไปอย่างปลอดภัยโดยให้ใช้วิธีการใส่ซองปิดผนึก จากนั้นจึงส่งให้กับผู้ใช้งานโดยตรง
- 4) ผู้ใช้งานต้องตอบยืนยันการได้รับรหัสผ่าน
- 5) เมื่อมีผู้ใช้งานระบบสารสนเทศของหน่วยงานลาออก หรือไม่มีหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิการใช้งาน ให้หน่วยงานแจ้งผู้ดูแลระบบสารสนเทศทันที เพื่อเปลี่ยนสิทธิหรือถอดสิทธิของผู้ที่ลาออกจากระบบทันทีที่ได้รับแจ้ง
- 6) ผู้ดูแลระบบสารสนเทศจัดทำระบบที่เอื้อให้ผู้ใช้งานสามารถเปลี่ยนรหัสผ่านของตนเองได้ โดยกำหนดให้เปลี่ยนทุก 180 วัน
- 7) ผู้ดูแลระบบสารสนเทศต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดได้ไม่เกิน 5 ครั้ง

### 4. การใช้งานโปรแกรมมอรรลประโยชน์ (Use of System Utilities)

- 1) ให้แยกโปรแกรมมอรรลประโยชน์ออกจากงานสารสนเทศ
- 2) จำกัดการใช้งานโปรแกรมมอรรลประโยชน์ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- 3) ให้บันทึกรายละเอียดการใช้งานโปรแกรมมอรรลประโยชน์
- 4) ห้ามติดตั้งโปรแกรมที่ละเมิดลิขสิทธิ์ ต้องใช้โปรแกรมที่ถูกลิขสิทธิ์เท่านั้น
- 5) ต้องติดตั้งโปรแกรมตามภารกิจและติดตั้งโปรแกรมที่เกี่ยวข้องกับการปฏิบัติงาน

### 5. การบริหารจัดการ Software และ ลิขสิทธิ์

- 1) สสวท. ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น Software ที่หน่วยงานอนุญาตให้ใช้งาน หรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่และความจำเป็น รวมถึงห้ามมิให้ผู้ใช้งานทำการติดตั้งหรือใช้งาน Software ที่มีการละเมิดลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

- 2) โปรแกรมที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงานห้ามมิให้ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อไปใช้งานที่อื่น ยกเว้นได้รับการอนุญาตจากผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมายที่มีสิทธิในเรื่องลิขสิทธิ์
- 3) ผู้ใช้งานต้องพึงระวังโปรแกรมประสงค์ร้าย (Malware) ได้แก่ virus, worms, spyware ตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติให้ผู้ใช้งานแจ้งกับผู้ดูแลระบบสารสนเทศโดยทันที
- 4) ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ของหน่วยงาน หรือของผู้อื่นโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ใช้สำหรับการประชุมจัดทำนโยบาย แนวปฏิบัติ PDPA สสวท. เท่านั้น



## ส่วนที่ 6

### การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

#### (Application and Information Access Control)

##### 1. การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ

- 1) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ผู้ใช้งานใหม่ปฏิบัติตามแนวปฏิบัติในหมวดที่ 1 การควบคุมการเข้าถึงระบบสารสนเทศ ส่วนที่ 1 การบริหารจัดการการเข้าถึงของผู้ใช้งาน ได้แก่
  - การลงทะเบียนผู้ใช้งานใหม่ (User Registration)
  - การบริหารสิทธิของผู้ใช้งานในการใช้งานระบบ (Privilege Management)
  - การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)
  - การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right)
- 2) การเข้าถึงแอปพลิเคชันผ่านทางเครือข่ายของ สสวท. ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนผู้ใช้งานที่ปลอดภัยโดยใช้ Username และ Password
- 3) การเข้าถึงแอปพลิเคชันผ่านทางเครือข่ายของสาธารณะให้ใช้ช่องทาง Secure Sockets Layer Virtual Private Network: SSL VPN และต้องมีการพิสูจน์ตัวตนผู้ใช้งานที่ปลอดภัยโดยใช้ Username และ Password
- 4) ผู้ดูแลระบบสารสนเทศต้องตัดเวลาการใช้งานเครื่องลูกข่าย เมื่อเครื่องลูกข่ายนั้นไม่ได้มีการใช้งานเป็นระยะเวลา 15 นาที (Session Time-out)
- 5) ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ระบบสารสนเทศจำกัดเวลาการเชื่อมต่อ (Limitation of Connection Time) สำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้ 2 ชั่วโมงต่อการเชื่อมต่อ 1 ครั้ง สำหรับผู้บริหาร และ 1 ชั่วโมงต่อครั้งสำหรับพนักงาน ทั้งนี้จะต้องมีการระบุตัวตนเพื่อการเข้าใช้งานใหม่ตามช่วงเวลาที่กำหนดไว้
- 6) ผู้ดูแลระบบสารสนเทศต้องบันทึกข้อมูลพฤติกรรมการใช้งานข้อมูลโดยจัดเก็บ Audit Log เป็น Log File ที่ใช้เก็บข้อมูลการเข้าถึงระบบของผู้ใช้งาน เพื่อตรวจสอบว่าใครเข้ามาใช้งานในระบบการตรวจสอบการบุกรุก
- 7) ในกรณีมีการจ้างพนักงาน Outsource เพื่อดำเนินการในเรื่องต่าง กำหนดมาตรการในการควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศไว้ดังนี้
  - กำหนดให้มีเจ้าหน้าที่ผู้ควบคุมงานเพื่อคอยกำกับดูแลการดำเนินงานต่าง ๆ ของพนักงาน Outsource

- แจ้งให้พนักงาน Outsource รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- กำหนดให้พนักงาน Outsource ลงนามสัญญารักษาความลับ
- ผู้ดูแลระบบสารสนเทศต้องกำหนดให้ Outsource ปฏิบัติตามแนวปฏิบัติในหมวดที่ 1 การควบคุมการเข้าถึงระบบสารสนเทศ ส่วนที่ 1 การควบคุมการเข้าถึงสารสนเทศ ส่วนที่ 2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

## 2. กำหนดคุณสมบัติการ Login ที่มีความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ

- 1) ไม่มีหรือไม่แสดง Function ให้ความช่วยเหลือระหว่างที่ทำการ Login
- 2) บันทึกความพยายามในการ Login ทั้งที่สำเร็จและไม่สำเร็จและแสดงประวัติการ Login 3 ครั้งล่าสุด
- 3) ตัดการเชื่อมต่อหลังจากที่ Login ไม่ประสบความสำเร็จเกินกว่า 3 ครั้ง
- 4) เมื่อมีการใส่ข้อมูลบัญชีผู้ใช้งานและรหัสผ่านที่ไม่ถูกต้อง ให้แสดงข้อความรวมๆ ได้แก่ “ข้อมูลการ login ไม่ถูกต้อง”
- 5) ให้แสดงข้อความเตือนที่หน้าจอหลังจากการ Login เสร็จสิ้น
- 6) ไม่แสดงรายละเอียดของระบบใด ๆ จนกว่าการ Login สำเร็จ

## 3. การแยกระบบสารสนเทศที่มีความสำคัญสูง

- 1) ระบบที่มีความสำคัญต่อองค์กรสูงต้องถูกแยกออกจากระบบสารสนเทศอื่นๆ ได้แก่ ระบบเงินเดือน ระบบประเมินผลพนักงาน ระบบข้อสอบและเฉลย เป็นต้น
- 2) ระบบที่มีความสำคัญต่อองค์กรสูงไม่อนุญาตให้เข้าถึงผ่านอุปกรณ์สื่อสารเคลื่อนที่ หรือการปฏิบัติงานจากภายนอกได้
- 3) ต้องจัดทำสำรองของระบบสารสนเทศที่มีความสำคัญสูงต่อองค์กร ตามแนวปฏิบัติหมวดที่ 2 การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน
- 4) ผู้ดูแลระบบสารสนเทศต้องมีเครื่องมือ (Tools) เพื่อใช้สำหรับตรวจสอบสภาพพร้อมใช้งานของระบบสารสนเทศที่มีความสำคัญสูง ได้แก่ ระบบ Network Monitoring ระบบ Application Monitoring

## 4. การปฏิบัติงานจากภายนอกองค์กร (Teleworking)

- 1) กำหนดการเข้าถึงแอปพลิเคชันและสารสนเทศของ สสวท. ได้ 2 ช่องทางดังนี้
  - การเข้าถึงผ่านแอปพลิเคชันและสารสนเทศที่เปิดให้ใช้งานจากภายนอกได้โดยตรง ได้แก่ Website ของ สสวท. ระบบ e-Mail
  - การเข้าถึงแอปพลิเคชันและสารสนเทศของ สสวท. ผ่านระบบ SSL VPN

- 2) ผู้ใช้งานได้รับสิทธิการเข้าใช้งานระบบสารสนเทศจากภายนอกหน่วยงานดังข้อ 1) ข้างต้น ดังแสดงในแนวปฏิบัติหมวดที่ 1 การควบคุมการเข้าถึงระบบสารสนเทศ ส่วนที่ 1 การควบคุมการเข้าถึงสารสนเทศ ข้อ 2 การบริหารสิทธิผู้ใช้งานในระบบ (Privilege Management) ซึ่งสามารถเข้าใช้งานได้โดยใช้ Username และ Password ของตนเอง
- 3) ในกรณีที่ผู้ใช้งานเป็น Outsource หรือบุคคลภายนอกต้องได้รับอนุญาตจาก ฝ่ายเทคโนโลยีสารสนเทศ ก่อนการเข้าใช้งาน ซึ่งสามารถเข้าใช้งานได้โดยการใช้ Username และ Password ที่ตนเองได้รับ
- 4) ผู้ดูแลระบบสารสนเทศต้องกำหนดสิทธิการเข้าถึงแอปพลิเคชันและสารสนเทศให้ผู้ใช้งานเข้าถึงแต่เพียงบริการที่ได้รับอนุญาตเท่านั้น
- 5) อุปกรณ์คอมพิวเตอร์ที่เชื่อมต่อเข้ากับแอปพลิเคชันและระบบสารสนเทศผ่านช่องทางการปฏิบัติงานจากภายนอกองค์กร ต้องได้รับการติดตั้ง Anti-Virus ที่ได้รับการ Update อย่างสม่ำเสมอ และมีการ Update ระบบปฏิบัติการอย่างสม่ำเสมอ

ใช้สำหรับการประชุมจัดทำนโยบาย แนวปฏิบัติด้านความปลอดภัย

## ส่วนที่ 7

### การควบคุมการเข้าถึงเครื่องแม่ข่าย (Server)

1. การควบคุมการเข้าถึงเครื่องแม่ข่ายให้เป็นไปตามแนวปฏิบัติหมวดที่ 1 การควบคุมการเข้าถึงระบบสารสนเทศ ส่วนที่ 1 การควบคุมการเข้าถึงสารสนเทศ ส่วนที่ 2 การบริหารจัดการการเข้าถึงผู้ใช้งาน ส่วนที่ 4 การควบคุมการเข้าถึงระบบเครือข่าย ส่วนที่ 5 การควบคุมการเข้าถึงระบบปฏิบัติการ และ ส่วนที่ 6 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ
2. การควบคุมการเข้าถึงเครื่องแม่ข่ายทางด้านกายภาพให้เป็นไปตามแนวปฏิบัติหมวดที่ 1 การควบคุมการเข้าถึงระบบสารสนเทศ ส่วนที่ 8 เรื่องความมั่นคงปลอดภัยด้านกายภาพ (Physical Security)

ใช้สำหรับการประชุมจัดทำนโยบาย แนวปฏิบัติ PDPA ส่วนที่ 7

## ส่วนที่ 8

### ความมั่นคงปลอดภัยด้านกายภาพ

#### (Physical Security)

#### 1. การรักษาความปลอดภัยด้านกายภาพ (Physical Security management)

- 1) กำหนดระดับความสำคัญของพื้นที่หรือจำแนกพื้นที่การใช้งาน
- 2) พื้นที่ที่มีระบบสารสนเทศอยู่ภายใน ได้แก่ Data Center ให้ติดตั้งสัญญาณเตือนภัยเพื่อแจ้งเตือนเมื่อมีการบุกรุก
- 3) ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพเพื่อตรวจสอบว่ายังใช้งานได้ตามปกติ
- 4) ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้กำหนดแนวปฏิบัติสำหรับควบคุมการเข้าถึงอุปกรณ์สารสนเทศขณะไม่มีผู้ใช้บริการ เพื่อป้องกันอุปกรณ์ขณะไม่มีผู้ใช้งานอุปกรณ์ โดยกำหนดข้อปฏิบัติดังนี้
  - หากมีพนักงานตรวจพบอุปกรณ์สารสนเทศที่ถูกละทิ้งโดยไม่มีผู้ใช้งานใกล้เคียง ให้แจ้งผู้ดูแลระบบสารสนเทศเพื่อป้องกันการโจรกรรมข้อมูลจากผู้ไม่ประสงค์ดีต่อไป
  - ผู้ใช้งานต้องปิดประตูหน้าต่างของพื้นที่ที่มีการติดตั้งระบบสารสนเทศให้ล็อกอยู่เสมอ เมื่อไม่มีผู้ใช้งาน
  - ผู้ใช้งานต้องป้องกันมิให้ผู้อื่นสามารถเข้าใช้อุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ระบบสารสนเทศของตนโดยต้องใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งาน
  - ผู้ใช้งานต้อง logout ออกจากระบบสารสนเทศทันทีเมื่อเสร็จสิ้นการใช้งานหรือไม่อยู่ที่หน้าอุปกรณ์คอมพิวเตอร์เป็นเวลานาน

#### 2. การควบคุมการเข้า - ออก (Physical Entry Control) โดยผู้ดูแลระบบสารสนเทศต้องควบคุมการเข้า-ออก ดังต่อไปนี้

- 1) ให้มีการบันทึกเวลาเข้า-ออก ของบุคคลที่เข้าพื้นที่สำคัญ
- 2) มีกลไกการอนุญาตการเข้าถึงพื้นที่ของบุคคลภายนอก
- 3) มีการควบคุมพื้นที่ที่มีข้อมูลสำคัญหรือประมวลผล
- 4) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่เว้นแต่ได้รับอนุญาต
- 5) มีการพิสูจน์ตัวตน ได้แก่ แสดงบัตรผ่าน การใช้แถบแม่เหล็ก การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออก ในพื้นที่หรือบริเวณที่มีความสำคัญ โดยเฉพาะ Data Center
- 6) บุคคลภายนอกต้องติดบัตรให้เห็นเด่นชัดจนตลอดเวลาอยู่ภายใน สสวท.

- 7) จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกขณะปฏิบัติงานภายในพื้นที่หรือบริเวณที่มีความสำคัญ
- 8) จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ
- 9) ห้ามถ่ายภาพบริเวณที่มีความสำคัญ ได้แก่ ห้อง Server เป็นต้น

### 3. การจำกัดบริเวณสำหรับการเข้าถึงหรือส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access Delivery and Loading Area)

- 1) จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายอุปกรณ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- 2) จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่ส่งมอบนั้น
- 3) จัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหาก เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในสสวท.
- 4) ให้ตรวจสอบวัสดุที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน
- 5) ตรวจสอบและลงทะเบียนหรือขึ้นบัญชีคอมพิวเตอร์ที่ส่งมอบโดยผู้ถูกจ้าง ผู้ขาย หรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุ

### 4. การจัดวางหรือการป้องกันอุปกรณ์ (Equipment Siting and Protection)

- 1) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อให้เกิดความเป็นระเบียบเรียบร้อย
- 2) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในอีกพื้นที่หนึ่งที่มีความมั่นคงปลอดภัย
- 3) ไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ที่มีระบบสารสนเทศ
- 4) ดำเนินการตรวจสอบ และดูแลสภาพแวดล้อมของพื้นที่ที่มีระบบสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ ได้แก่ การตรวจสอบระดับอุณหภูมิ ความชื้น เป็นต้น

### 5. ระบบและอุปกรณ์สนับสนุนการทำงาน ( Supporting Utilities)

- 1) มีระบบและอุปกรณ์สนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการทำงานดังต่อไปนี้
  - ระบบสำรองไฟฟ้า (UPS)
  - เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
  - ระบบระบายอากาศ
  - ระบบปรับอากาศ และควบคุมความชื้น
  - ระบบดับเพลิง

- 2) ให้ใช้เครื่องกำเนิดกระแสไฟฟ้าสำรองสำหรับ Data Center เพื่อจ่ายไฟสำรองให้ทั้งในระดับเครื่องแม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์สนับสนุน ในกรณีที่กระแสไฟฟ้าหลักเกิดการหยุดชะงักหรือดับเป็นระยะเวลายาวนาน
- 3) กำหนดให้จัดทำแผนฉุกเฉินสำหรับ เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบระบายอากาศ ระบบปรับอากาศ ระบบควบคุมความชื้น และระบบดับเพลิง
- 4) ให้จัดทำสวิตช์ฉุกเฉินไว้ใกล้กับบริเวณทางออกของห้องเครื่อง เพื่อให้สามารถปิดสวิตช์ดับอุปกรณ์ทั้งหมดได้โดยทันทีทันใดและอย่างรวดเร็ว
- 5) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนอย่างสม่ำเสมอ เพื่อลดความเสี่ยงความล้มเหลวในการทำงานของระบบ
- 6) ติดตั้งระบบแจ้งเตือนในพื้นที่สำคัญ เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

#### 6. การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling Security)

- 1) สายเคเบิลที่ต้องวางผ่านเข้าไปบริเวณที่มีบุคคลภายนอกเข้าถึงได้นั้น ต้องมีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายเพื่อก่อให้เกิดความเสียหาย รวมถึงป้องกันสัตว์ต่าง ๆ มากัดสาย
- 2) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน
- 3) ทำป้ายชื่อกำกับสายสัญญาณ และอุปกรณ์ เพื่อป้องกันการติดต่อสัญญาณผิดเส้น
- 4) จัดทำแผงฝังสัญญาณสื่อสารต่างๆ ให้ครบถ้วนถูกต้อง
- 5) ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ให้ปิดสลักให้สนิท เพื่อป้องกันการเข้าถึงจากบุคคลภายนอก

#### 7. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

- 1) ให้กำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด
- 2) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ
- 3) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง
- 4) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
- 5) ควบคุมและสอดส่องดูแลการปฏิบัติงานของบริษัทผู้รับเหมาบำรุงรักษาระบบคอมพิวเตอร์ ที่มาทำการบำรุงรักษาอุปกรณ์ภายใน สสวท.

- 6) ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- 7) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่บำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

#### 8. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of Equipment Off-Premises)

- 1) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำสิ่งอุปกรณ์ หรือทรัพย์สินของ สสวท. ออกไปใช้นอกสำนักงาน
- 2) ไม่ทิ้งสิ่งอุปกรณ์หรือทรัพย์สินของ สสวท. ไว้ลำพังในที่สาธารณะ
- 3) ให้ผู้ที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินของ สสวท. เสมือนเป็นทรัพย์สินของตนเอง

#### 9. การจำกัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้อีกครั้ง (Secure Disposal or Reuse of Equipment)

- 1) ให้ทำลายข้อมูลในอุปกรณ์ก่อนที่จะดำเนินการจำหน่ายอุปกรณ์ดังกล่าว
- 2) ใช้วิธีการทำลายข้อมูลตามแนวปฏิบัติ หมวดที่ 1 การควบคุมการเข้าถึงระบบสารสนเทศ ส่วนที่ 3 หน้าที่รับผิดชอบของผู้ใช้งาน ข้อที่ 4. การทำลายสื่อข้อมูลอิเล็กทรอนิกส์ ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์ตัวนั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เข้าถึงข้อมูลนั้นได้

#### 10. การนำทรัพย์สินออกนอกสำนักงาน (Removal of Property)

- 1) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือสินทรัพย์ออกนอกสำนักงาน
- 2) บันทึกการนำอุปกรณ์ออกนอกสำนักงานและบันทึกการส่งคืน เพื่อเก็บไว้เป็นหลักฐานป้องกันการสูญหาย



เอกสารหมวดที่ 2

การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน

(Backup and IT Continuity Plan)

ส่วน	เรื่อง	หน้า
ส่วนที่ 1	การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan)	29

ใช้สำหรับการประชุมจัดทำนโยบาย แนวปฏิบัติ PDPA สวท. เท่านั้น

## หมวดที่ 2

### การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน

#### (Backup and IT Continuity Plan)

#### วัตถุประสงค์

1. เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สำหรับการใช้งานได้อย่างต่อเนื่อง มีประสิทธิภาพ และในเวลาที่ต้องการ โดยกำหนดแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์รวมทั้งการทดสอบการเก็บรักษา จัดทำและการทดสอบแผนฉุกเฉิน

#### ผู้รับผิดชอบ

1. ฝ่ายเทคโนโลยีสารสนเทศ
2. ผู้ดูแลระบบ

#### ขอบเขต

แนวปฏิบัติในหมวดนี้ครอบคลุมถึง พนักงาน และบุคคลภายนอกที่มีการดำเนินการเกี่ยวกับระบบสารสนเทศของ สสวท.

## ส่วนที่ 1

### การสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน

#### (Backup and IT Continuity Plan)

#### 1. การสำรองข้อมูลและกู้คืนข้อมูลกำหนดให้ใช้แนวปฏิบัติในการจัดทำนโยบายการสำรองและกู้คืนข้อมูลดังต่อไปนี้

- 1) กำหนดให้จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน และจัดทำระบบสำรองที่เหมาะสม และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง
- 2) กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้นโดยให้มีวิธีการสำรองข้อมูล ดังนี้
  - กำหนดประเภท และความถี่ในการสำรองของข้อมูล อย่างน้อยต้องประกอบด้วยข้อมูลจากฐานข้อมูลของระบบ ค่าคอนฟิกูเรชันของระบบ และของระบบปฏิบัติการที่ใช้
  - กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง
  - บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้รับผิดชอบ ผู้ดำเนินการ วัน/เวลา ขนาดข้อมูลที่สำรอง ความสำเร็จ หรือข้อผิดพลาด
  - จัดเก็บข้อมูลที่สำรองไว้ในอีกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรอง กับหน่วยงานควรห่างกันเพียงพอไม่ให้เกิดผลกระทบต่อข้อมูลที่จัดเก็บไว้ในอีกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน
  - จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
  - ตรวจสอบและทดสอบการกู้คืนข้อมูลให้เป็นไปตามข้อกำหนดของแผนที่ได้กำหนดไว้ ซึ่งรวมถึงเวลากู้คืนระบบ และปริมาณข้อมูลสูญหายที่ยอมรับได้

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย  
ให้ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศและผู้ดูแลระบบเครือข่ายให้กำกับดูแลการสำรองข้อมูลดังนี้

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล	ความถี่ในการตรวจสอบสื่อบันทึกข้อมูล	ผู้รับผิดชอบ
อุปกรณ์เครือข่าย Network Equipment	ค่า Configuration Policies Rules	- รายสัปดาห์ (เป็นปกติ) - ก่อนและหลังการเปลี่ยนแปลง	- 6 เดือนต่อครั้ง (แบบสุ่ม) - ปีละครั้ง (แบบสมบูรณ์)	- ผู้ดูแลระบบสำรองข้อมูล - ผู้ดูแลระบบเครือข่าย
ฐานข้อมูลของแต่ละระบบงาน	- ค่า Configuration ของระบบปฏิบัติการ	- รายสัปดาห์ (เป็นปกติ) - ก่อนและหลังการเปลี่ยนแปลง	- 6 เดือนต่อครั้ง (แบบสุ่ม) - ปีละครั้ง (แบบสมบูรณ์)	- ผู้ดูแลระบบสำรองข้อมูล - ผู้ดูแลฐานข้อมูลในแต่ละระบบ
	- ฐานข้อมูล	- ทุกวัน เวลา 24:00 (เป็นปกติ) - ก่อนและหลังการเปลี่ยนแปลง	- 6 เดือนต่อครั้ง (แบบสุ่ม) - ปีละครั้ง (แบบสมบูรณ์)	- ผู้ดูแลระบบสำรองข้อมูล - ผู้ดูแลฐานข้อมูลในแต่ละระบบ
	- Log ฐานข้อมูล	- ทุกวัน เวลา 24:00 (เป็นปกติ) - ก่อนและหลังการเปลี่ยนแปลง	- 6 เดือนต่อครั้ง (แบบสุ่ม) - ปีละครั้ง (แบบสมบูรณ์)	- ผู้ดูแลระบบสำรองข้อมูล - ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์
ระบบจดหมายอิเล็กทรอนิกส์	- ค่า Configuration ของระบบปฏิบัติการ	- รายสัปดาห์ (เป็นปกติ) - ก่อนและหลังการเปลี่ยนแปลง	- 6 เดือนต่อครั้ง (แบบสุ่ม) - ปีละครั้ง (แบบสมบูรณ์)	- ผู้ดูแลระบบสำรองข้อมูล - ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์
	- ค่า Configuration ของ MS-Exchange	- ก่อนและหลังการเปลี่ยนแปลง	- 6 เดือนต่อครั้ง (แบบสุ่ม) - ปีละครั้ง (แบบสมบูรณ์)	- ผู้ดูแลระบบสำรองข้อมูล - ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์
	- ฐานข้อมูล (Exchange DB) - Exchange DB Log	- ทุกวัน เวลา 24:00 (เป็นปกติ) - ก่อนและหลังการเปลี่ยนแปลง	- 6 เดือนต่อครั้ง (แบบสุ่ม) - ปีละครั้ง (แบบสมบูรณ์)	- ผู้ดูแลระบบสำรองข้อมูล - ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์
ระบบ Web Server	- ค่า Configuration ของระบบปฏิบัติการ	- รายเดือน (เป็นปกติ) - ก่อนและหลังการเปลี่ยนแปลง	- 6 เดือนต่อครั้ง (แบบสุ่ม) - ปีละครั้ง (แบบสมบูรณ์)	- ผู้ดูแลระบบสำรองข้อมูล - ผู้ดูแลระบบ Web Server
	- ค่า Configuration ของ Web Service	- ก่อนและหลังการเปลี่ยนแปลง	- 6 เดือนต่อครั้ง (แบบสุ่ม) - ปีละครั้ง (แบบสมบูรณ์)	- ผู้ดูแลระบบสำรองข้อมูล - ผู้ดูแลระบบ Web Server
ระบบ File Sharing SharePoint	ข้อมูลบน Website ที่เผยแพร่	- รายเดือน (เป็นปกติ) - ก่อนและหลังการเปลี่ยนแปลง	- 6 เดือนต่อครั้ง (แบบสุ่ม) - ปีละครั้ง (แบบสมบูรณ์)	- ผู้ดูแลระบบสำรองข้อมูล - ผู้ดูแลระบบ Web Server
	- ค่า Configuration ของระบบปฏิบัติการ	- รายสัปดาห์ (เป็นปกติ) - ก่อนและหลังการเปลี่ยนแปลง	- 6 เดือนต่อครั้ง (แบบสุ่ม) - ปีละครั้ง (แบบสมบูรณ์)	- ผู้ดูแลระบบสำรองข้อมูล - ผู้ดูแลระบบ SharePoint
	- ค่า Configuration ของ Files Service - ค่า Configuration ของ SharePoint	- ก่อนและหลังการเปลี่ยนแปลง	- 6 เดือนต่อครั้ง (แบบสุ่ม) - ปีละครั้ง (แบบสมบูรณ์)	- ผู้ดูแลระบบสำรองข้อมูล - ผู้ดูแลระบบ SharePoint

ตารางที่ 2 : วิธีการกำกับดูแลการสำรองข้อมูล

- 3) การสำรองข้อมูลนอกเหนือจากข้อกำหนดข้างต้น การกำหนดความถี่ในการสำรองข้อมูล ขึ้นอยู่กับความสำคัญของข้อมูลและการยอมรับความเสี่ยงที่กำหนดโดยผู้รับผิดชอบข้อมูล หรือผู้รับผิดชอบระบบ
- 4) กำหนดขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง ครอบคลุมทั้งส่วนอุปกรณ์และซอฟต์แวร์
- 5) ข้อมูลที่สำรองไว้ต้องได้รับกระบวนการพิสูจน์ความสมบูรณ์ครบถ้วนของข้อมูลที่สำรองทุกครั้ง
- 6) จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้คืนระบบกลับคืนได้ภายในระยะเวลาที่กำหนด
- 7) การสำรองข้อมูลและการกู้ข้อมูลของทุกระบบ ต้องถูกบันทึกเป็นเอกสาร และมีการตรวจสอบความถูกต้องเป็นระยะ ๆ
- 8) ต้องตรวจสอบรายงานบันทึกการจัดเก็บสื่อข้อมูลที่สถานที่จัดเก็บข้อมูลสำรองเป็นประจำทุกปี หรือตามความเหมาะสม
- 9) สื่อบันทึกข้อมูลสำรองต้องมีการเปลี่ยนตามอายุการใช้งานและประเภทของสื่อ

2. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง

อิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุง แผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

- 1) จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียด ตามแผนความพร้อมกรณีฉุกเฉินฯ ซึ่งครอบคลุมหัวข้อดังนี้
  - กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
  - ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยง ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว และการชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้
  - กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และการทดสอบกู้คืนข้อมูลที่สำรองไว้
  - กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ
  - การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน
- 2) ทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้ อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจอย่างน้อยปีละ 1 ครั้ง

3. ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1 ครั้ง
4. ทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ 1 ครั้ง

ใช้สำหรับการประชุมจัดทำนโยบาย แนวปฏิบัติ PDPA สลวท. เท่านั้น

เอกสารหมวดที่ 3

การตรวจสอบและประเมินความเสี่ยง

ส่วน	เรื่อง	หน้า
ส่วนที่ 1	การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	34

ใช้สำหรับการประชุมจัดทำนโยบาย แนวปฏิบัติ PDPA สลวท. เท่านั้น

### หมวดที่ 3

#### การตรวจสอบและประเมินความเสี่ยง

##### วัตถุประสงค์

1. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศและลดความเสี่ยงที่อาจเกิดขึ้นได้กับระบบสารสนเทศ

##### ผู้รับผิดชอบ

1. ฝ่ายเทคโนโลยีสารสนเทศ
2. ผู้ตรวจสอบภายใน
3. ผู้ตรวจสอบภายนอก
4. ผู้ดูแลระบบที่ได้รับมอบหมาย

##### ขอบเขต

แนวปฏิบัติในหมวดนี้ครอบคลุมถึง พนักงาน และบุคคลภายนอกที่มีการดำเนินการเกี่ยวกับระบบสารสนเทศของ สสวท.

ใช้สำหรับการประชุมจัดทမ်းนโยบาย แนวปฏิบัติ PDPA สสวท. เท่านั้น



## ส่วนที่ 1

### การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

#### 1. การตรวจสอบและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Assessment)

1) ฝ่ายเทคโนโลยีสารสนเทศ สสวท. ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

- ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ 1 ครั้ง
- ตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงาน โดยดำเนินการอย่างน้อยปีละ 1 ครั้ง
- ตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายนอกหน่วยงาน โดยดำเนินการอย่างน้อย 2 ปีครั้ง

2) แนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึงอย่างน้อย ดังนี้

- ทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ 1 ครั้ง
- ทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ 1 ครั้ง
- ตรวจสอบ ประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
- มีมาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อย ดังนี้
  - กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้  
อย่างเดียว
  - ในกรณีที่จำเป็นในการเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น  
เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ

เอกสารหมวดที่ 4

แนวปฏิบัติอื่นๆ

ส่วน	เรื่อง	หน้า
ส่วนที่ 1	การใช้งานคอมพิวเตอร์ส่วนบุคคล อุปกรณ์คอมพิวเตอร์โน้ตบุ๊ก และอุปกรณ์คอมพิวเตอร์ (Use of Personal Computer , Notebook , and Computer Devices )	36
ส่วนที่ 2	การใช้งานอินเทอร์เน็ต (Internet Usage)	38
ส่วนที่ 3	สื่อสังคมออนไลน์ (Social Media)	40
ส่วนที่ 4	การใช้งาน e-Mail (Use of e-Mail)	42
ส่วนที่ 5	การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	43

ใช้สำหรับการประชุมจัดทำนโยบาย PDPA สวท. เท่านั้น

## หมวดที่ 4

### แนวปฏิบัติอื่นๆ

#### วัตถุประสงค์

1. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย
2. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

#### ผู้รับผิดชอบ

1. ฝ่ายเทคโนโลยีสารสนเทศ
2. ผู้ใช้งาน

#### ขอบเขต

แนวปฏิบัติในหมวดนี้ครอบคลุมถึง พนักงาน และบุคคลภายนอกที่มีการดำเนินการเกี่ยวกับระบบสารสนเทศของ สสวท.

ใช้สำหรับการประชุมจัดทำนโยบาย แนวปฏิบัติ PDPA สสวท. เท่านั้น

## ส่วนที่ 1

### การใช้งานคอมพิวเตอร์ส่วนบุคคล อุปกรณ์คอมพิวเตอร์โน้ตบุ๊ก และอุปกรณ์คอมพิวเตอร์

(Use of Personal Computer Notebook and Computer Devices)

#### 1. แนวทางปฏิบัติในการใช้งานทั่วไป

- 1) อุปกรณ์คอมพิวเตอร์ที่อนุญาตให้ผู้ใช้ นำไปงานเป็นสินทรัพย์ของ สสวท. ดังนั้นผู้ใช้งานจะต้องใช้งานอย่างมีประสิทธิภาพ เพื่อดำเนินงานก่อให้เกิดหน่วยงาน เท่านั้น
- 2) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของ สสวท. ต้องเป็นโปรแกรมที่ทาง สสวท. ได้ซื้ออย่างถูกกฎหมาย ดังนั้นห้ามให้ผู้ใช้งานทำการคัดลอกโปรแกรมตลงๆ และนำไปติดตั้งบนคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปใช้โดยผิดกฎหมาย
- 3) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในอุปกรณ์คอมพิวเตอร์ส่วนบุคคลของหน่วยงานก่อนได้รับอนุญาตจากฝ่ายเทคโนโลยีสารสนเทศ
- 4) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งอุปกรณ์คอมพิวเตอร์ใดๆ เข้าไปในระบบเครือข่ายคอมพิวเตอร์ ก่อนได้รับอนุญาต
- 5) การเคลื่อนย้ายหรือส่งอุปกรณ์คอมพิวเตอร์ส่วนบุคคลตรวจสอบจะต้องดำเนินการโดยเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ หรือเจ้าหน้าที่ที่มีความรับผิดชอบระบบสารสนเทศนั้น
- 6) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบ เพื่อหา Virus โดยโปรแกรม Anti-Virus
- 7) ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่อง
- 8) ให้ผู้ใช้งานปฏิบัติตามแนวทางการจัดการรหัสผ่าน ตามแนวปฏิบัติการใช้งานรหัสผ่านอย่างปลอดภัย

#### 2. การป้องกันจากโปรแกรมหรือชุดคำสั่งประสงค์ร้าย (Malware)

- 1) ผู้ใช้งานต้องตรวจสอบหา Virus จากสื่อต่างๆ ก่อนนำมาใช้งาน ได้แก่ Flash drive และ Data Storage เป็นต้น
- 2) ผู้ใช้งานต้องตรวจสอบ File ที่แนบมากับ e-Mail หรือ File ที่ได้จากการ Download จากอินเทอร์เน็ตด้วยโปรแกรม Anti-Virus ก่อนนำมาใช้งาน
- 3) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งประสงค์ร้ายรวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลบนคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นๆ ได้รับความเสียหาย ถูกทำลาย แก้ไข

แก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงกับคำสั่งที่กำหนดไว้ หากพบให้แจ้งกับฝ่ายเทคโนโลยีสารสนเทศให้ทราบทันที

### 3. การสำรองและการกู้คืน

- 1) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากอุปกรณ์คอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ ได้แก่ CD , DVD , External Harddisk
- 2) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้สถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

### 4. การขออนำอุปกรณ์หรือเครื่องคอมพิวเตอร์ส่วนบุคคลที่มีได้เป็นทรัพย์สินของ สสวท. เชื่อมต่อกับอุปกรณ์หรือระบบคอมพิวเตอร์ของ สสวท.

- 1) ให้ผู้ใช้งานหรือหน่วยงานที่ร้องขอดำเนินการกรอกแบบฟอร์มการลงทะเบียนนำอุปกรณ์ หรือระบบคอมพิวเตอร์เชื่อมต่อกับระบบเครือข่ายของ สสวท. นำเสนอต่อผู้อำนวยการฝ่าย/สาขา/โครงการ เพื่อพิจารณาในเบื้องต้น แล้วนำเสนอฝ่ายเทคโนโลยีสารสนเทศต่อไป
  - กรณีที่ขอเชื่อมต่อกับระบบเครือข่ายที่อยู่ในความดูแลของฝ่ายเทคโนโลยีสารสนเทศ ให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้พิจารณาเห็นชอบ
  - กรณีที่ขอเชื่อมต่อกับระบบที่ไม่ได้อยู่ในความดูแลของฝ่ายเทคโนโลยีสารสนเทศ ให้ผู้อำนวยการฝ่าย/สาขา/โครงการ ที่กำกับดูแลระบบเป็นผู้พิจารณาเห็นชอบ
- 2) เมื่อผู้ใช้งานหรือหน่วยงานที่ร้องขอได้รับอนุญาตแล้ว ให้สามารถนำอุปกรณ์หรือระบบคอมพิวเตอร์มาเชื่อมต่อกับระบบเครือข่ายของ สสวท. ได้ โดยฝ่ายเทคโนโลยีสารสนเทศจะประสานงานกับผู้ร้องขอเพื่อทำการตั้งค่าระบบรวมถึงโปรแกรมต่างๆที่จำเป็นต่อไป
- 3) เมื่อต้องการเปลี่ยนแปลงวิธีการ รูปแบบการเชื่อมต่อ หรือสิ่งอื่นใดที่ผิดไปจากที่ร้องขอไว้ ให้แจ้งฝ่ายเทคโนโลยีสารสนเทศทราบก่อนดำเนินการเปลี่ยนแปลงใดๆ ทั้งนี้ฝ่ายเทคโนโลยีสารสนเทศจะเป็นผู้พิจารณาเพื่อพิจารณาดำเนินการตามข้อ 1) เมื่อได้รับความเห็นชอบแล้วจึงสามารถดำเนินการเปลี่ยนแปลงได้

## ส่วนที่ 2

### การใช้งานอินเทอร์เน็ต

#### (Internet Usage)

#### 1. แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

- 1) ผู้ดูแลระบบเครือข่ายกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์กับอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย ได้แก่ Proxy Firewall เป็นต้น
- 2) อุปกรณ์คอมพิวเตอร์ส่วนบุคคลและอุปกรณ์คอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตต้องติดตั้งโปรแกรม Anti-Virus
- 3) ผู้ใช้งานต้องไม่ใช้ระบบเครือข่ายอินเทอร์เน็ตของ สสวท. เพื่อหาผลประโยชน์ในเชิงธุรกิจส่วนตัวและเข้าสู่ Website ที่ไม่เหมาะสม ได้แก่ Website ที่ขัดต่อศีลธรรม เป็นต้น
- 4) ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของ สสวท. โดยผ่านความเห็นชอบจากผู้บังคับบัญชา
- 5) ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับของ สสวท. โดยไม่ได้รับอนุญาตอย่างเป็นทางการผ่านระบบเครือข่ายอินเทอร์เน็ต
- 6) ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน
- 7) ผู้ใช้งานอินเทอร์เน็ตต้องทำการ Login ด้วย Username และ Password ของตนเองก่อนการใช้งานทุกครั้ง และให้ทำการ Logout ทุกครั้งเมื่อสิ้นสุดการใช้งาน เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ
- 8) ผู้ใช้งานต้องปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 อย่างเคร่งครัด

#### 2. มาตรการป้องกันและรักษาความปลอดภัยจากการเชื่อมต่ออินเทอร์เน็ตความเร็วสูง

- 1) การขอเปิดใช้บริการเชื่อมต่ออินเทอร์เน็ตความเร็วสูง ผ่านโทรศัพท์หมายเลขเอกชน หน่วยงานผู้ขอใช้จะต้องเสนอขออนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ผ่านฝ่ายเทคโนโลยีสารสนเทศเพื่อพิจารณาความเหมาะสมและความจำเป็นต่อไป

- 2) การเชื่อมต่ออินเทอร์เน็ตความเร็วสูง จะต้องไม่เชื่อมต่อกับอุปกรณ์คอมพิวเตอร์ของ สสวท. ที่เชื่อมต่อกับระบบ Intranet หรือเครื่องคอมพิวเตอร์ส่วนตัวที่มีข้อมูลข่าวสารของ สสวท. ที่เป็นชั้นความลับโดยเด็ดขาด

### 3. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์

ผู้ดูแลระบบสารสนเทศต้องจัดเก็บข้อมูลการจราจรคอมพิวเตอร์ กรณีที่มีบริการเข้าถึงระบบอินเทอร์เน็ตจากภายในหน่วยงานโดยจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นไปตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และตามประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเรื่อง “หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550”

ใช้สำหรับการประชุมจัดทำนโยบาย แนวปฏิบัติ PDPA สสวท. เก็บข้อมูล

### ส่วนที่ 3

#### สื่อสังคมออนไลน์

##### (Social Media)

#### 1. การใช้สื่อสังคมออนไลน์ทั่วไป

- 1) สสวท. อนุญาตให้ใช้ระบบเครือข่ายเพื่อเข้าถึงสื่อสังคมออนไลน์ที่ไม่ได้มีเนื้อหาที่ขัดต่อกฎหมาย ศีลธรรม และหลักจรรยาบรรณของ สสวท.
- 2) หน่วยงานภายในของ สสวท. บุคลากร สามารถแสดงชื่อผู้ใช้งานในโลกออนไลน์เพื่อประโยชน์ในการเผยแพร่ ประชาสัมพันธ์ที่เกี่ยวข้องกับองค์กรติดต่อกับสื่อสารระหว่างกัน แต่จะต้องแยกแยะว่าข้อความใดให้ชัดเจน ได้แก่ “ข่าวประชาสัมพันธ์” “ข้อคิดเห็น” “ความเห็นส่วนตัว” “การแลกเปลี่ยนข่าวสารส่วนตัว” เป็นต้น
- 3) การเผยแพร่ประชาสัมพันธ์ที่ประชาสัมพันธ์ในนามของหน่วยงาน ผู้เผยแพร่ต้องแสดงตำแหน่ง หน้าที่ ให้ชัดเจน เพื่อความน่าเชื่อถือ และเพื่อให้ผู้ติดตามสามารถใช้ดุลพินิจในการติดตามได้
- 4) ให้ระมัดระวังการใช้ถ้อยคำ ภาษาที่ใช้ ที่อาจเป็นการดูหมิ่น หรือหมิ่นประมาทผู้อื่น ควรใช้ภาษาที่ถูกต้อง มีความสุภาพ สร้างสรรค์
- 5) งดเว้นการใช้สื่อสังคมออนไลน์วิพากษ์วิจารณ์ ตลอดจนแสดงความคิดเห็นในเรื่องที่เป็นข้อมูลภายในของ สสวท. หรืออาจส่งผลกระทบต่อ สสวท. ได้
- 6) การใช้สื่อสังคมออนไลน์จะต้องไม่รบกวนการปฏิบัติงานหรือหน้าที่ความรับผิดชอบ

#### 2. การใช้สื่อสังคมออนไลน์ ในระดับองค์กร

- 1) การจัดทำสื่อสังคมออนไลน์ ควรจะคำนึงถึงเรื่องดังต่อไปนี้
  - วัตถุประสงค์ในการจัดทำ
  - แนวทางการใช้งานสื่อสังคมออนไลน์เพื่อพัฒนาและดำเนินการของ สสวท.
- 2) การใช้ชื่อหรือตราสัญลักษณ์ของ สสวท. เพื่อเปิดบัญชีผู้ใช้งานผ่านสื่อสังคมออนไลน์ โดยมีวัตถุประสงค์เพื่อการประชาสัมพันธ์ เผยแพร่ข้อมูลข่าวสาร หรือสื่อสารกันภายในองค์กร จะต้องผ่านการรับทราบและเห็นชอบจาก CIO และต้องคำนึงถึงหลักการใช้อินเทอร์เน็ตทั่วไปข้างต้น
- 3) การนำเสนอข่าวโดยใช้อินเทอร์เน็ตขององค์กร ควรมีหลักในการอ้างอิงถึงองค์กรดังต่อไปนี้
  - ชื่อองค์กรที่เผยแพร่ข้อมูลข่าวสาร



- รายละเอียด สัญลักษณ์ หรือชื่อย่อ ที่แสดงถึงองค์กร
  - มาตรการทางเทคนิคที่ยืนยันถึงการมีตัวตนขององค์กร
  - ชื่อตัวแทนองค์กรที่นำเสนอข่าวสาร (ถ้ามี)
- 4) ในกรณีที่มีบัญชีผู้ใช้งานของ สสวท. ควรมีการตั้งค่า privacy เพื่อป้องกันมิให้บุคคลอื่นทำการ Post ข้อความ หรือ เข้าถึงข้อมูลที่มีความสำคัญหรือเป็นความลับ ซึ่งห้ามเปิดเผยโดยอัตโนมัติ โดยมีการกำหนดให้อยู่ในวงจำกัดเท่านั้น และควรระวังในการ Post ข้อความเฉพาะกลุ่มหรือส่วนบุคคลไม่ต้องการให้เผยแพร่สู่สาธารณชนรับรู้
  - 5) การนำเสนอข้อมูลข่าวสารขององค์กรผ่านทางสื่อสังคมออนไลน์ ควรเป็นไปตามจริยธรรมหลักเกณฑ์ และไม่สร้างความเกลียดชัง จนนำไปสู่ความขัดแย้งขึ้นในสังคม
  - 6) สสวท. ต้องให้ความเคารพและยอมรับข่าวสาร หรือภาพข่าวที่ผลิตโดยบุคคลอื่นผ่านสื่อสังคมออนไลน์ การคัดลอกข้อมูล ได้แก่ ข้อความ รูปภาพ เป็นต้น พึงได้รับอนุญาตจากเจ้าของนั้นๆ ตามแต่กรณี และต้องอ้างอิงถึงแหล่งที่มาของสื่อเหล่านั้นโดยรับรู้ถึงสิทธิ หรือ ลิขสิทธิ์ขององค์กรหรือบุคคลผู้เป็นผู้รับผิดชอบข้อมูลดังกล่าว
  - 7) ไม่นำข้อมูลที่เป็นความลับทุกระดับชั้นขององค์กรมาเผยแพร่ผ่านช่องทางสื่อสังคมออนไลน์ทุกประเภท

## ส่วนที่ 4

### การใช้งาน e-Mail

#### (Use of e-Mail)

#### 1. แนวทางปฏิบัติในการส่ง e-Mail

- 1) ผู้ดูแลระบบ e-Mail ต้องกำหนดสิทธิการเข้าถึงระบบ e-Mail ของ สสวท. ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานรวมทั้งทบทวนสิทธิการเข้าใช้งานอยู่เสมอ ได้แก่ การเปลี่ยนตำแหน่ง เปลี่ยนต้นสังกัด ลาออก เกษียณอายุ
- 2) ผู้ดูแลระบบ e-Mail ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบ e-Mail
- 3) ผู้ใช้งานต้องกำหนดรหัสผ่านที่ดี (Good Password) ตามแนวปฏิบัติการใช้งานรหัสผ่านอย่างปลอดภัย
- 4) ผู้ใช้งานต้องตรวจสอบเนื้อหาก่อนทำการส่ง e-Mail ได้แก่ e-Mail ของผู้รับ เนื้อหาในจดหมาย เป็นต้น
- 5) ผู้ใช้งานต้องใช้ e-Mail เพื่อใช้ติดต่อกับงานของ สสวท. เท่านั้น
- 6) ผู้ใช้งานต้องลบ e-Mail ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ของระบบ e-Mail
- 7) ผู้ใช้งานต้องทำการตรวจสอบ File ที่แนบมากับ e-Mail ก่อนทำการเปิดใช้งานเพื่อตรวจสอบข้อมูล โดยใช้โปรแกรม Anti-Virus เป็นการป้องกันในการเปิด File จำพวก Executable ได้แก่ .exe .pif .bat .cmd .com เป็นต้น
- 8) หลังจากการใช้งาน e-Mail เสร็จสิ้น ผู้ใช้งานต้องทำการ Logout ทุกครั้ง เพื่อเป็นการป้องกันบุคคลอื่นเข้าใช้งาน e-Mail

## ส่วนที่ 5

### การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

#### 1. การสร้างความตระหนัก การให้ความรู้ และการอบรมด้านความมั่นคงปลอดภัยให้แก่พนักงาน

- 1) จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมโดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนฝึกอบรมพนักงานของ สสวท.
- 2) ดำเนินการประชาสัมพันธ์ในรูปแบบต่างๆ ในการให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปสู่การปฏิบัติได้ง่าย
- 3) ระดมการมีส่วนร่วมและนำไปสู่การปฏิบัติด้านการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ใช้สำหรับการประชุมจัดทำนโยบาย แนวปฏิบัติ PDPA สสวท.

เอกสารหมวดที่ 5

บททั่วไป

ส่วน	เรื่อง	หน้า
ส่วนที่ 1	แนวปฏิบัติเมื่อเกิดปัญหาหรือข้อขัดแย้ง	44

ใช้สำหรับการประชุมจัดทำนโยบาย แนวปฏิบัติ PDPA สสวท. เท่านั้น

หมวดที่ 5

บททั่วไป

วัตถุประสงค์

1. เพื่อกำหนดผู้วินิจฉัยชี้ขาด เมื่อเกิดปัญหาหรือข้อขัดแย้งในการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ 1

แนวปฏิบัติเมื่อเกิดปัญหาหรือข้อขัดแย้ง

1. เมื่อเกิดปัญหาหรือข้อขัดแย้งในการปฏิบัติตามแนวปฏิบัตินี้ ให้ผู้อำนวยการวินิจฉัยชี้ขาด
2. ให้ถือคำวินิจฉัยชี้ขาดถือเป็นแนวปฏิบัติต่อไป

ประกาศ ณ วันที่ 3 สิงหาคม พ.ศ. 2559



(นางพรพรรณ ไวทยานุกร)

ผู้อำนวยการสถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี

ใช้สำหรับการประชุมจัดทำนโยบาย แนวปฏิบัติ PDPA สสวท. เท่านั้น