นโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศ

พ.ศ.
2569

ความลับ
(Confidentiality)

ความถูกต้อง
(Integrity)

ความพร้อมใช้งาน
(Availability)

สำนักเทคโนโลยีสารสนเทศ
สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

นโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของ
สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

พฤษภาคม 2569

ประวัติเอกสาร

เวอร์ชัน	วันที่	ผู้แก้ไข	สิ่งที่แก้ไข/ดำเนินการ
1.0	26 ธันวาคม 2555	นายบุญเกียรติ สวัสดิ์โชติชวลิต	ได้รับความเห็นชอบจาก คณะกรรมการธุรกรรม อิเล็กทรอนิกส์
1.1	21 พฤษภาคม 2557	นายบุญเกียรติ สวัสดิ์โชติชวลิต	ทบทวนครั้งที่ 1 ประจำปี 2557
2.0	กันยายน 2562	นายเฟาซี เจ๊ะเต๊ะ	ทบทวนครั้งที่ 2 ประจำปี 2562
2.1	สิงหาคม 2563	นายเฟาซี เจ๊ะเต๊ะ	ทบทวนครั้งที่ 3 ประจำปี 2563
2.2	พฤษภาคม 2566	นายเฟาซี เจ๊ะเต๊ะ	ทบทวนครั้งที่ 4 ประจำปี 2566
2.3	เมษายน 2567	นายเฟาซี เจ๊ะเต๊ะ	ทบทวนครั้งที่ 5 ประจำปี 2567
2.4	เมษายน 2568	นายเฟาซี เจ๊ะเต๊ะ	ทบทวนครั้งที่ 6 ประจำปี 2568
2.5	พฤษภาคม 2569	นายเฟาซี เจ๊ะเต๊ะ	ทบทวนครั้งที่ 7 ประจำปี 2569

คำนำ

ในยุคปัจจุบัน เทคโนโลยีสารสนเทศและการสื่อสารมีบทบาทสำคัญอย่างยิ่งต่อการดำเนินงานของสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) หรือ พอช. ข้อมูลและระบบสารสนเทศถือเป็นทรัพย์สินที่มีค่าและเป็นหัวใจหลักในการขับเคลื่อนภารกิจของสถาบันฯ เพื่อสนับสนุนการสร้างความเข้มแข็งขององค์กรชุมชนและประชาสังคมทั่วประเทศ เพื่อให้การบริหารจัดการข้อมูลและระบบสารสนเทศของสถาบันฯ เป็นไปด้วยความเรียบร้อย มีมาตรฐาน ปลอดภัย และสอดคล้องกับกฎหมาย ระเบียบ และข้อบังคับที่เกี่ยวข้อง สถาบันฯ จึงได้จัดทำ “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” ฉบับนี้ขึ้น เพื่อใช้เป็นกรอบแนวทางสำหรับเจ้าหน้าที่ ผู้ปฏิบัติงานของสถาบันฯ ที่เกี่ยวข้องกับข้อมูลและระบบสารสนเทศของสถาบันฯ ได้ยึดถือและปฏิบัติตาม

เอกสารฉบับนี้ได้กำหนดหลักเกณฑ์และมาตรการที่จำเป็นในการป้องกัน คุ้มครอง และจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ครอบคลุมทั้งในด้านบุคลากร กระบวนการ เทคโนโลยี และสภาพแวดล้อมทางกายภาพ เพื่อเป็นแนวทางในการใช้งานระบบสารสนเทศระบบสารสนเทศของสถาบันฯ ใช้งานได้อย่างเหมาะสม สนับสนุนการดำเนินงานของสถาบันฯ ได้อย่างต่อเนื่อง มีประสิทธิภาพ บรรลุตามวิสัยทัศน์และพันธกิจที่ตั้งไว้ สำนักเทคโนโลยีสารสนเทศ มุ่งหวังให้ทุกส่วนงานที่เกี่ยวข้องตระหนักถึงความสำคัญและให้ความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัตินี้อย่างเคร่งครัด เพื่อเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยด้านสารสนเทศที่เข้มแข็ง และเป็นรากฐานสำคัญในการพัฒนางานขององค์กรชุมชนอย่างยั่งยืนสืบไป

สำนักเทคโนโลยีสารสนเทศ

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

1. หลักการและเหตุผล

สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) เล็งเห็นถึงความสำคัญของระบบข้อมูลสารสนเทศและเทคโนโลยีดิจิทัลซึ่งเป็นเครื่องมือสนับสนุนการปฏิบัติงานและการบริหารงานได้อย่างมีประสิทธิภาพ และโดยที่มีการประกาศบังคับใช้กฎหมายที่เกี่ยวกับการพัฒนารัฐบาลดิจิทัลของรัฐบาลได้แก่ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐ พ.ศ.2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันจึงได้จัดทำนโยบายและแนวปฏิบัติฉบับนี้ขึ้น เพื่อใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยของระบบข้อมูลสารสนเทศของสถาบันให้มีความมั่นคงปลอดภัยและเชื่อถือได้ สอดคล้องกับกฎหมายที่เกี่ยวข้อง

2. ความหมายและขอบเขตของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายและแนวปฏิบัติของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้จัดทำขึ้นเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศซึ่งครอบคลุมการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบข้อมูลที่อยู่ในความรับผิดชอบของสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) ในขอบเขตดังต่อไปนี้

2.1 การรักษาความมั่นคงปลอดภัยของการเข้าถึงข้อมูลและระบบข้อมูล ตลอดจนควบคุมการใช้งานระบบสารสนเทศ ซึ่งครอบคลุมการเข้าถึง 4 ด้าน ได้แก่

2.1.1 การเข้าถึงระบบเทคโนโลยีสารสนเทศ (Information Access Control)

2.1.2 การเข้าถึงระบบเครือข่าย (Network Access control)

2.1.3 การเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

2.1.4 การเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (Application Access Control)

2.2 การจัดให้มีการสำรองข้อมูลสารสนเทศที่สำคัญอย่างสม่ำเสมอ เพื่อให้อยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

2.3 การตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละครั้ง

3. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3.1 การพิจารณาถึงความสำคัญของข้อมูลและระบบข้อมูลต่อพันธกิจและนโยบายของหน่วยงานและสนับสนุนการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบข้อมูลที่สำคัญ และครอบคลุมขอบเขตที่กฎหมายกำหนด

3.2 การเผยแพร่ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานเองและของหน่วยงานที่เกี่ยวข้อง

3.3 การบริหารจัดการความต่อเนื่องของภารกิจที่หน่วยงานรับผิดชอบ

3.4 การมีแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสม กรณีมีการละเมิดหรือฝ่าฝืนนโยบายความมั่นคงปลอดภัย

3.5 การนิยามและกำหนดความรับผิดชอบของบุคลากรที่เกี่ยวข้อง ซึ่งประกอบด้วย

3.5.1 ระดับนโยบาย รับผิดชอบในการกำหนดนโยบาย แนวทางและมาตรการด้านต่าง ๆ ที่เกี่ยวกับการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร ตลอดจนมาตรการเกี่ยวกับการรักษาความปลอดภัยของข้อมูล ได้แก่ ผู้อำนวยการ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของสถาบันพัฒนาองค์กรชุมชน คณะทำงานพัฒนาระบบข้อมูลสารสนเทศและเทคโนโลยีดิจิทัลและหัวหน้าสำนักเทคโนโลยีสารสนเทศ

3.5.2 ระดับปฏิบัติ รับผิดชอบในการปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และปฏิบัติหน้าที่อื่น ๆ ตามที่ได้รับมอบหมาย ได้แก่ ผู้ดูแลระบบ และ ผู้ปฏิบัติงาน

3.6 การจัดทำหรือปรับปรุงนโยบายและแนวทางปฏิบัติ ควรมีการระบุความเสี่ยง มีการประเมินและกำหนดแนวทางจัดการความเสี่ยงนั้น ๆ โดยการประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

3.6.1 ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

3.6.2 ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

3.6.3 จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

3.7 การปรับปรุงนโยบายและแนวปฏิบัติ ให้มีการทบทวนปรับปรุงอย่างน้อยปีละครั้ง

3.8 กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายอันตรายใด ๆ แก่สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้ผู้บริหารระดับสูงสุดเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

4. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำหรับแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นการจัดทำเอกสารเพื่อกำหนดแนวทางวิธีการในการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องเป็นไปตามนโยบายที่กำหนดไว้ และสามารถนำไปอ้างอิงปฏิบัติได้ โดยแบ่งแนวปฏิบัติออกเป็นส่วน ๆ ดังนี้

ส่วนที่ 1 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ 2 แนวปฏิบัติการควบคุมการเข้าออกห้องสำนักเทคโนโลยีสารสนเทศ

ส่วนที่ 3 แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 4 แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 5 แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

ส่วนที่ 6 แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์แบบพกพา
ส่วนที่ 7 แนวปฏิบัติการใช้งานอินเทอร์เน็ต
ส่วนที่ 8 แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์
ส่วนที่ 9 แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
ส่วนที่ 10 แนวปฏิบัติในการสำรองข้อมูล
ส่วนที่ 11 แนวปฏิบัติในการสร้างความต่อเนื่องให้กับธุรกิจ
ส่วนที่ 12 แนวปฏิบัติในการประเมินความเสี่ยงเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ส่วนที่ 13 แนวปฏิบัติการกำหนดพื้นที่เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ
ส่วนที่ 14 แนวปฏิบัติการบริหารจัดการรหัสผ่าน
ส่วนที่ 15 แนวปฏิบัติการบริหารจัดการสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ
ส่วนที่ 16 แนวปฏิบัติการบริหารจัดการครุภัณฑ์คอมพิวเตอร์และเครือข่าย
ส่วนที่ 17 แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ส่วนที่ 18 แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย
ส่วนที่ 19 แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล
ส่วนที่ 20 แนวปฏิบัติการควบคุมแอพพลิเคชั่น
ส่วนที่ 21 แนวปฏิบัติการกำหนดมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ
ส่วนที่ 22 แนวปฏิบัติการใช้งาน GENERATIVE AI
ส่วนที่ 23 แนวปฏิบัติการใช้งานระบบคลาวด์ (CLOUD SERVICE)

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

1. สถาบัน หมายความว่า สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

2. ผู้อำนวยการ หมายความว่า ผู้อำนวยการสถาบันพัฒนาองค์กรชุมชน

3. ผู้บังคับบัญชา หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสถาบัน

4. สำนักเทคโนโลยีสารสนเทศ หมายความว่า ส่วนงานที่มีหน้าที่ดูแลระบบสารสนเทศของสถาบันตามโครงสร้างของสถาบัน

5. ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หมายความว่า ผู้ที่ผู้อำนวยการแต่งตั้งให้ดำรงตำแหน่งหรือรักษาการ

6. ผู้ใช้งาน หมายความว่า บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของสถาบันโดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งสถาบันกำหนดไว้ ได้แก่ ผู้บริหาร ผู้ดูแลระบบ ผู้ปฏิบัติงาน องค์กรชุมชน เครือข่ายองค์กรชุมชน และหน่วยงานภายนอก

7. ผู้บริหาร หมายความว่า ผู้มีอำนาจบริหารในระดับสูงของสถาบัน

8. ผู้ดูแลระบบ (System Administrator) หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

9. ผู้ปฏิบัติงาน หมายความว่า ผู้ปฏิบัติงานตามความในมาตรา 32 แห่งพระราชกฤษฎีกาจัดตั้งสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) พ.ศ. 2543

10. องค์กรชุมชน หมายความว่า กลุ่มคนที่มีระบบการจัดการที่สมาชิกของชุมชนจัดตั้งขึ้นเพื่อดำเนินการร่วมกัน โดยมีวัตถุประสงค์เพื่อประโยชน์ในการประกอบอาชีพ พัฒนาอาชีพ เพิ่มรายได้ พัฒนาที่อยู่อาศัยและสิ่งแวดล้อมหรือพัฒนาชีวิตความเป็นอยู่ของสมาชิกในกลุ่ม

11. เครือข่ายองค์กรชุมชน หมายความว่า กลุ่มองค์กรชุมชนที่มีการรวมตัวกันโดยมีวัตถุประสงค์ที่จะกระทำกิจการอย่างหนึ่งอย่างใด เพื่อประโยชน์ขององค์กรชุมชนในกลุ่มนั้น

12. หน่วยงานภายนอก หมายความว่า องค์กรหรือหน่วยงานภายนอกที่สถาบัน อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของสถาบัน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

13. สิทธิของผู้ใช้งาน หมายความว่า สิทธิของผู้ใช้ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยมีการอนุญาตให้เฉพาะผู้ที่เกี่ยวข้องและมีความจำเป็น

14. ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

15. สารสนเทศ (Information) หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

16. ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

17. ระบบเครือข่าย (Network System) หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของสถาบันได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

17.1 ระบบแลน (LAN) และ ระบบอินทราเน็ต (Intranet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

17.2 ระบบอินเทอร์เน็ต (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

17.3 ระบบเครือข่ายไร้สาย (Wireless Lan) หมายความว่า ระบบการสื่อสารข้อมูลที่มีรูปแบบในการสื่อสารแบบไม่ใช้สาย โดยใช้การส่งคลื่นความถี่วิทยุ ในการรับและส่งข้อมูลระหว่างคอมพิวเตอร์แต่ละเครื่อง

18. ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

19. พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายความว่า พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

19.1 พื้นที่ทำงานทั่วไป (General working area) หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน

19.2 พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)

19.3 พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)

19.4 พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)

19.5 พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

20. เจ้าของข้อมูล หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

21. สินทรัพย์ หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

22. จดหมายอิเล็กทรอนิกส์ (e-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

23. รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

24. ชุดคำสั่งไม่พึงประสงค์ (Malware) หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้ เช่น ไวรัส (virus), เวิร์ม (Worm) หรือหนอนคอมพิวเตอร์, มาโทรจัน (Trojan), สปายแวร์ (Spyware) เป็นต้น

25. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การควบคุมบุคคลที่ไม่ได้รับอนุญาตในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบัน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก

26. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบัน ให้เป็นไปตามหลักของการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

27. เหตุการณ์ด้านความมั่นคงปลอดภัย หมายความว่า เหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบันทำให้ระบบข้อมูลไม่มีความมั่นคงปลอดภัย หรือสร้างความเสียหายให้แก่สถาบันได้ในลักษณะใดลักษณะหนึ่ง ดังนี้

27.1 เกิดการหยุดชะงักต่อกระบวนการสำคัญทางธุรกิจ

27.2 ละเมิดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสถาบัน

27.3 ละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่าง ๆ ที่สถาบันกำหนดไว้

27.4 ทำให้สถาบันสูญเสียชื่อเสียง

28. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของสถาบันถูกบุกรุกโจมตี และคุกคามความมั่นคงปลอดภัย

29. การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

30. ภัยคุกคามทางไซเบอร์ (cyber threats) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

31. ไซเบอร์ (Cyber) หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

32. หน่วยงานของรัฐ หมายความว่า ราชการส่วนกลาง ราชการส่วนภูมิภาค ราชการส่วนท้องถิ่น รัฐวิสาหกิจ องค์กรฝ่ายนิติบัญญัติ องค์กรฝ่ายตุลาการ องค์กรอิสระ องค์การมหาชน และหน่วยงานอื่นของรัฐ

33. ประมวลแนวทางปฏิบัติ หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กาหนด

34. เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

35. มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

36. โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

37. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

38. หน่วยงานควบคุมหรือกำกับดูแล หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคล ซึ่งมีกฎหมายกาหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

39. ดิจิทัล หมายความว่า เทคโนโลยีที่ใช้วิธีการนำสัญลักษณ์ศูนย์และหนึ่ง หรือสัญลักษณ์อื่นมาแทนค่าสิ่งทั้งปวง เพื่อใช้สร้างหรือก่อให้เกิดระบบต่าง ๆ เพื่อให้มนุษย์ใช้ประโยชน์

40. รัฐบาลดิจิทัล หมายความว่า การนำเทคโนโลยีดิจิทัลมาใช้เป็นเครื่องมือในการบริหารงานภาครัฐและการบริการสาธารณะ โดยปรับปรุงการบริหารจัดการและบูรณาการข้อมูลภาครัฐและการทำงานให้มีความสอดคล้องและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล เพื่อเพิ่มประสิทธิภาพ และอำนวยความสะดวกในการให้บริการประชาชน ในการเปิดเผยข้อมูลภาครัฐต่อสาธารณชน และสร้างการมีส่วนร่วมของทุกภาคส่วน

41. คอมไพเลอร์ หมายความว่า โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น

42. แพตช์ หมายความว่า โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update

43. Recovery Time Objective (RTO) หมายความว่า ระยะเวลาในการกู้คืนระบบ

44. Recovery Point Objective (RPO) หมายความว่า ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

45. Maximum Tolerance Period of Disruption (MTPD) หมายความว่า ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่นภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด

46. ระบบคลาวด์ (Cloud Service) หมายความว่า การให้บริการด้านระบบคอมพิวเตอร์ ระบบจัดเก็บข้อมูล ระบบเครือข่าย ระบบประมวลผล หรือบริการด้านเทคโนโลยีสารสนเทศผ่านเครือข่ายอินเทอร์เน็ต โดยผู้ให้บริการภายนอก ซึ่งผู้ใช้งานสามารถเข้าถึงและใช้งานทรัพยากรสารสนเทศได้ตามสิทธิที่กำหนด

47. ผู้ให้บริการระบบคลาวด์ (Cloud Service Provider) หมายความว่า หน่วยงานหรือองค์กรภายนอกที่ให้บริการระบบคลาวด์หรือโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศแก่สถาบัน

48. ปัญญาประดิษฐ์ (Artificial Intelligence : AI) หมายความว่า ระบบหรือโปรแกรมคอมพิวเตอร์ที่สามารถประมวลผล วิเคราะห์ สร้างเนื้อหา หรือสนับสนุนการตัดสินใจโดยอาศัยแบบจำลองหรืออัลกอริทึมอัตโนมัติ

49. Generative AI หมายความว่า ระบบปัญญาประดิษฐ์ที่สามารถสร้างข้อความ ภาพ เสียง วิดีโอ โปรแกรมคอมพิวเตอร์ หรือเนื้อหาอื่นในรูปแบบดิจิทัลจากข้อมูลหรือคำสั่งที่ได้รับ

50. ข้อมูลส่วนบุคคล หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

51. ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) หมายความว่า ข้อมูลส่วนบุคคลที่กฎหมายกำหนดให้ต้องได้รับความคุ้มครองเป็นพิเศษ เช่น เชื้อชาติ ศาสนา ข้อมูลสุขภาพ ข้อมูลชีวภาพ หรือข้อมูลทางการเงิน

52. การพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA) หมายความว่า กระบวนการยืนยันตัวตนโดยใช้ปัจจัยมากกว่าหนึ่งรูปแบบ เช่น รหัสผ่าน รหัส OTP หรืออุปกรณ์ยืนยันตัวตน

53. การเข้ารหัสข้อมูล (Encryption) หมายความว่า กระบวนการแปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้โดยไม่ได้รับอนุญาต เพื่อป้องกันการเข้าถึงข้อมูลโดยมิชอบ

54. การสำรองข้อมูล (Backup) หมายความว่า กระบวนการทำสำเนาข้อมูลหรือระบบสารสนเทศเพื่อใช้ในการกู้คืนข้อมูลหรือระบบในกรณีเกิดความเสียหาย สูญหาย หรือหยุดชะงัก

55. การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) หมายความว่า กระบวนการวางแผน เตรียมความพร้อม และกำหนดแนวทางรองรับเหตุการณ์ที่อาจส่งผลกระทบต่อการดำเนินงาน เพื่อให้หน่วยงานสามารถดำเนินภารกิจสำคัญได้อย่างต่อเนื่อง

แนวปฏิบัติการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการด้านความมั่นคงปลอดภัยไซเบอร์สำหรับข้อมูลและระบบสารสนเทศของหน่วยงาน ให้เป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามไซเบอร์ รวมถึงสร้างความเชื่อมั่นในการดำเนินงานอย่างต่อเนื่องและปลอดภัย

2. ขอบเขต

นโยบายนี้ครอบคลุมข้อมูลและระบบสารสนเทศทุกประเภทของหน่วยงาน รวมถึงบุคลากร ผู้ใช้งาน อุปกรณ์ และกระบวนการที่เกี่ยวข้องกับการจัดการข้อมูลและระบบสารสนเทศ

3. คุณลักษณะความมั่นคงปลอดภัยไซเบอร์ที่ต้องมี

- **ความลับ (Confidentiality):** ข้อมูลต้องได้รับการปกป้องไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงหรือเปิดเผย
- **ความสมบูรณ์ (Integrity):** ข้อมูลต้องถูกต้อง ครบถ้วน ไม่มีการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
- **ความพร้อมใช้งาน (Availability):** ข้อมูลและระบบสารสนเทศต้องพร้อมใช้งานเมื่อจำเป็น
- **ความรับผิดชอบ (Accountability):** สามารถตรวจสอบและระบุผู้กระทำในระบบได้
- **การพิสูจน์ตัวตน (Authentication):** ผู้ใช้งานต้องผ่านกระบวนการยืนยันตัวตนก่อนเข้าถึงระบบ

4. มาตรการและแนวปฏิบัติ

- **การประเมินและบริหารความเสี่ยง:**
    - ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ
- **การควบคุมการเข้าถึง:**
    - กำหนดสิทธิ์การเข้าถึงข้อมูลและระบบตามหน้าที่
    - ใช้หลัก Least Privilege และแยกหน้าที่สำคัญ
    - มีการควบคุมการเข้าถึงเครือข่ายและระบบปฏิบัติการ รวมถึงการพิสูจน์ตัวตนสำหรับผู้ใช้งานภายนอก
- **การสำรองข้อมูลและแผนกู้คืน:**
    - สำรองข้อมูลอย่างสม่ำเสมอและทดสอบการกู้คืนข้อมูล
    - จัดทำแผนเตรียมความพร้อมในกรณีฉุกเฉิน
- **การตรวจสอบและเฝ้าระวัง:**
    - มีระบบตรวจจับและแจ้งเตือนเหตุการณ์ผิดปกติ
    - เฝ้าระวังภัยคุกคามทั้งจากภายในและภายนอก

- **การตอบสนองและฟื้นฟู:**
    - กำหนดกระบวนการรับมือและฟื้นฟูเมื่อเกิดเหตุภัยคุกคาม
    - ทบทวนและปรับปรุงแผนรับมือและกู้คืนอย่างสม่ำเสมอ
- **การสร้างความตระหนักรู้:**
    - จัดอบรมและสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคลากรทุกระดับ
- **การบำรุงรักษาและอัปเดต:**
    - อัปเดตซอฟต์แวร์และระบบอย่างสม่ำเสมอเพื่อป้องกันช่องโหว่

5. การทบทวนและปรับปรุงนโยบาย

นโยบายนี้ต้องได้รับการทบทวนและปรับปรุงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงทางเทคโนโลยี กฎหมาย หรือภัยคุกคามใหม่ ๆ

ส่วนที่ 1
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งาน และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

2. แนวปฏิบัติทั่วไป

2.1 ภายในสถาบันมีการจำแนก และกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม ซึ่งกำหนดอยู่ใน *“แนวปฏิบัติการกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ”* (ส่วนที่ 13) เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

2.2 ผู้บริหารควรกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

2.3 ผู้บริหารควรกำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถมีสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน การกำหนดสิทธิประกอบด้วย

2.3.1 การจัดทำ *“แบบฟอร์มทะเบียนผู้มีสิทธิเข้า-ออกพื้นที่”* เพื่อเข้าใช้งานระบบเทคโนโลยีสารสนเทศ

2.3.2 การบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว

2.3.3 การจัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ และให้มีการปรับปรุงรายการผู้มีสิทธิเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

3. แนวปฏิบัติการควบคุมการเข้า-ออกอาคารสถานที่

3.1 ผู้ใช้งาน จะได้รับสิทธิให้เข้า-ออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

3.2 หากมีบุคคลอื่นใดที่ไม่ใช่ ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่ทางราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกรายชื่อบุคคล และการขอเข้าออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

4. แนวปฏิบัติการควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย

4.1 ข้อมูลที่สำคัญมาก เช่น ข้อมูลในกระดาษ ข้อมูลในสื่อหน่วยความจำสำรอง ควรได้รับการปกป้อง (เช่น ในตู้เซฟ หรือในตู้ และอื่น ๆ) เมื่อไม่จำเป็นต้องใช้และเมื่อมีการยกเลิกหรือพ้นจากตำแหน่ง

4.2 จุดรับเข้าและส่งออกจดหมาย และเครื่องโทรสารที่ไม่ได้ใช้งานควรได้รับการป้องกัน

4.3 เครื่องถ่ายเอกสารและอุปกรณ์ผลิตซ้ำแบบอื่น (เช่น เครื่องสแกนเนอร์ กล้องดิจิตอล) ควรได้รับการปกป้องจากการใช้งานที่ไม่ได้รับอนุญาต

4.4 เอกสารที่มีข้อมูลสำคัญควรนำออกจากเครื่องพิมพ์ทันที

ส่วนที่ 2
แนวปฏิบัติการควบคุมการเข้าออกห้องสำนักเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของสถาบัน โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องสำนักเทคโนโลยีสารสนเทศ

2. บทบาทและความรับผิดชอบ

2.1 ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

2.1.1 อนุมัติสิทธิเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

2.1.2 อนุมัติกระบวนการควบคุมการเข้า-ออกสำนักเทคโนโลยีสารสนเทศ

2.2 ผู้ดูแลระบบ

2.2.1 ตรวจสอบบุคคลที่ขออนุญาตเข้ามาภายในสำนักเทคโนโลยีสารสนเทศให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของสำนักเทคโนโลยีสารสนเทศ อย่างเคร่งครัด

2.2.2 ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกสำนักเทคโนโลยีสารสนเทศ ต้องติด *“บัตรผู้ติดต่อ”* หรือมีการยืนยันตัวตนว่าเป็นผู้ปฏิบัติงานของสถาบัน เท่านั้น

3. แนวปฏิบัติการควบคุมการเข้าออกห้อง

3.1 ผู้ดูแลระบบ และผู้ปฏิบัติงานสถาบัน มีแนวปฏิบัติดังนี้

3.1.1 ผู้ดูแลระบบ ควรจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนของงานระบบฐานข้อมูล ส่วนของงานระบบเทคโนโลยี เป็นต้น โดยจัดทำเป็น *“แนวปฏิบัติการกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ”* (ส่วนที่ 13) เพื่อสะดวกในการปฏิบัติงาน และยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

3.1.2 กรณีผู้ปฏิบัติงานที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้า-ออกสำนักเทคโนโลยีสารสนเทศ ก็ต้องมีการควบคุมอย่างรัดกุม

3.1.3 การเข้าถึงสำนักเทคโนโลยีสารสนเทศ และห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ต้องมีการลงบันทึกการเข้า-ออกไว้เป็นหลักฐาน

3.2 ผู้ติดต่อจากหน่วยงานภายนอก มีแนวปฏิบัติดังนี้

3.2.1 ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือ ใบอนุญาตขับขี่กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับ *“บัตรผู้ติดต่อ”*

3.2.2 ผู้ติดต่อจากหน่วยงานภายนอกต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในสำนักเทคโนโลยีสารสนเทศ

3.2.3 ผู้ติดต่อจากหน่วยงานภายนอกสามารถเข้า-ออกสำนักเทคโนโลยีสารสนเทศ ได้ด้วย *“บัตรผู้ติดต่อ”* โดยสิทธิจะขึ้นอยู่กับเหตุผลความจำเป็นในการขอเข้าปฏิบัติงานภายในสำนักเทคโนโลยีสารสนเทศ

ส่วนที่ 3
แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตในการเข้าถึงระบบเทคโนโลยีสารสนเทศของสถาบัน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของสถาบันได้อย่างถูกต้อง

2. หลักการในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

2.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้า-ออก ที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

2.2 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.3 ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

2.4 ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของสถาบัน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

2.5 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

3. แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1 ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐานตามที่ระบุใน *“แนวปฏิบัติการบริหารจัดการสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ”* (ส่วนที่ 15)

3.2 เจ้าของข้อมูลและเจ้าของระบบ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

3.3 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

4. แนวปฏิบัติการบริหารจัดการการเข้าถึงข้อมูลของผู้ใช้

4.1 การลงทะเบียนผู้มีสิทธิหรือยกเลิกสิทธิการใช้ระบบสารสนเทศของสถาบัน กรณีผู้ปฏิบัติงานต้องได้รับการจดแจ้งหรือรับรองเป็นลายลักษณ์อักษรจากหน่วยงานซึ่งมีหน้าที่ดูแลการจ้างงานของสถาบัน

4.2 กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบ รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ โดยเป็นไปตามที่ระบุใน *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน”* (ส่วนที่ 14)

4.3 การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน

4.3.1 ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

4.3.2 การกำหนด การเปลี่ยนแปลง และการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน”* (ส่วนที่ 14)

4.3.3 ต้องกำหนดให้ผู้ใช้เก็บรักษาเอกสารยอมรับที่จะเก็บรักษารหัสผ่านให้เป็นความลับเฉพาะตน และเก็บรหัสผ่านของกลุ่มไว้เฉพาะสมาชิกในกลุ่มเท่านั้น

4.3.4 การส่งรหัสผ่านชั่วคราวให้กับผู้ใช้ให้ใช้วิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลที่สามหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

4.3.5 ต้องกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

4.3.6 การกำหนดชื่อผู้ใช้หรือรหัส ID ต้องไม่ซ้ำกัน

4.3.7 กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยต้องปฏิบัติตาม *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน”* (ส่วนที่ 14)

4.3.7.1 ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานที่ต้องการ

4.3.7.2 ต้องควบคุมการใช้งานอย่างเข้มงวดโดยจัดสรรบนพื้นฐานของความจำเป็นเป็นครั้ง ๆ ไป เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

4.3.7.3 ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

4.3.7.4 ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานให้ทำการเปลี่ยนรหัสผ่านทุก 3 เดือน หรือกำหนดรหัสผ่านที่มั่นคง รัดกุม และปลอดภัย สอดคล้องตาม “แนวปฏิบัติการบริหารจัดการรหัสผ่าน” (ส่วนที่ 14)

4.3.7.5 ต้องมีการกำหนดให้ชัดเจนถึงสิทธิพิเศษที่ได้รับว่าการเข้าถึงแต่ละผลิตภัณฑ์ เช่น ซอฟต์แวร์ประเภทระบบปฏิบัติการ ระบบจัดการฐานข้อมูล และโปรแกรมประยุกต์แต่ละตัว สามารถเข้าถึงผลิตภัณฑ์ใดบ้าง

4.3.7.6 กระบวนการกำหนดสิทธิและการบันทึกการให้สิทธิพิเศษทั้งหมดต้องได้รับการดูแลพิเศษ โดยไม่จัดสรรให้จนกว่ากระบวนการขอสิทธิจะเสร็จสิ้นสมบูรณ์

4.3.7.7 สิทธิพิเศษของการเข้าถึงนั้นจะจำเป็นเฉพาะในกรณีพิเศษ เช่น เกิดความผิดพลาดในกระบวนการปฏิบัติงาน เป็นต้น

4.3.7.8 ส่งเสริมให้มีการพัฒนาและใช้โปรแกรมที่ไม่ใช้สิทธิพิเศษในการทำงาน

4.3.7.9 สิทธิพิเศษต้องได้รับการมอบหมายให้กับรหัสผู้ใช้งานที่ต่างจากรหัสผู้ใช้งานที่ใช้งานตามปกติ

4.4 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

4.4.1 ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

4.4.2 กำหนดรายชื่อผู้ใช้และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

4.5 ผู้ดูแลระบบ จะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ทุกครั้งที่มีการเปลี่ยนแปลงสิทธิและความรับผิดชอบ เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

4.6 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption หรือวิธีอื่นใดที่เหมาะสม

4.7 กำหนดให้มีการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ใน *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน”* (ส่วนที่ 14)

4.8 กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของสถาบัน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ผู้ใช้งานต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

5. แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ

5.1 ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal zone) โซนภายนอก (External zone) และโซนสำหรับเครื่องแม่ข่าย (DMZ zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

5.2 ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

5.3 ผู้ดูแลระบบต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน รวมทั้งตรวจสอบและปิดพอร์ต (Port) ของอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

5.4 ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

5.5 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ ตามความจำเป็น

5.6 ระบบเครือข่ายทั้งหมดของสถาบันที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสถาบันจะต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

5.7 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสถาบันในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

5.8 การเข้าสู่ระบบเครือข่ายและระบบสารสนเทศภายในสถาบัน โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ login เพื่อการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง และติดตามการเข้าใช้งานและกระบวนการกำหนดสิทธิ์การเข้าถึงหรือการใช้งานของผู้ใช้งาน (Authorization) โดยระบบจะตรวจสอบสิทธิ์ของผู้ใช้งานและกำหนดการเข้าถึงหรือการใช้งานที่เหมาะสมตามสิทธิ์ที่กำหนดไว้ให้

5.9 กำหนดประเภทของข้อมูล ช่องทางและเวลาในการเข้าถึง ดังต่อไปนี้

5.9.1 ข้อมูลที่ผู้ปฏิบัติงานสถาบัน สามารถเข้าถึงได้ตามสิทธิการใช้งานที่ได้รับอนุญาต สามารถใช้งานได้ผ่านระบบแลน (LAN) เครือข่ายไร้สาย (Wi-Fi) อินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet) คือข้อมูลที่อนุญาตให้เจ้าหน้าที่ของสถาบันสามารถเข้าถึงได้ตลอด 24 ชั่วโมง หรือในเวลาปฏิบัติงาน คือข้อมูลที่ที่เกี่ยวกับการปฏิบัติงาน

5.9.2 ข้อมูลที่ผู้ใช้งานที่ไม่ได้เป็นผู้ปฏิบัติงานของสถาบัน สามารถเข้าถึงข้อมูลที่เกี่ยวข้องกับการดำเนินงานของผู้ใช้งานตามสิทธิการใช้งานที่ได้รับอนุญาต โดยสามารถใช้งานได้ผ่านระบบอินเทอร์เน็ต (Internet) ได้ตลอด 24 ชั่วโมง ภายใต้โดเมน codi.or.th

5.10 IP address ภายในของระบบงานเครือข่ายภายในของสถาบัน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของสำนักเทคโนโลยีสารสนเทศได้โดยง่าย ซึ่งผู้ดูแลระบบเท่านั้นที่จะเป็นผู้กำหนด IP address ให้กับอุปกรณ์ต่าง ๆ (Fixed IP address)

5.11 เพื่อให้สามารถระบุอุปกรณ์บนเครือข่ายได้ จะต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ โดยใช้ IP address ในการระบุอุปกรณ์บนเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

5.12 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบและปรับแต่งระบบเครือข่าย จะต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานและช่องทางหรือพอร์ตเฉพาะที่จำเป็นเท่านั้น เช่น Telnet ftp หรือ ping เป็นต้น

5.13 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ เท่านั้น

6. แนวปฏิบัติการบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

6.1 กำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

6.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

6.3 ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ ftp หรือ ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

6.4 ดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server, App Server เป็นต้น

6.5 ดำเนินการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

6.6 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศเท่านั้น

6.7 การสำรองค่า config (Configuration Backup) เป็นกระบวนการที่เกี่ยวข้องกับการบันทึกข้อมูลการกำหนดค่า (configuration) ของระบบหรือแอปพลิเคชัน เพื่อใช้ในการเก็บไว้เป็นสำรองหากเกิดปัญหาหรือสูญเสียข้อมูลในการกำหนดค่าหลัก เพื่อให้สามารถกู้คืนการตั้งค่าได้ง่ายและรวดเร็วในกรณีที่เกิดความผิดพลาดหรือภัยคุกคามต่าง ๆ อีกทั้งยังช่วยให้สามารถเรียกคืนสถานะที่สมบูรณ์ของระบบหรือแอปพลิเคชันในกรณีที่เกิดข้อผิดพลาดร้ายแรงและต้องนำสถานะกลับมาใช้งานก่อนหน้าได้

7. แนวปฏิบัติการบริหารจัดการการบันทึกและตรวจสอบ

7.1 กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command line และ Firewall Log เป็นต้น เพื่อประโยชน์การใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน

7.2 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

8. แนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอกสถาบัน

สำนักเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในสถาบันเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกสถาบัน โดยมีแนวทางปฏิบัติดังนี้

8.1 การเข้าสู่ระบบจากระยะไกล (Remote Access) จะต้องเชื่อมต่อเครือข่ายผ่าน VPN เท่านั้น เนื่องเป็นการป้องกันระบบเครือข่ายคอมพิวเตอร์ของสถาบันที่อาจก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของสถาบัน การควบคุมบุคคลที่เข้าสู่ระบบของสถาบันจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

8.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

8.3 ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสถาบันอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

8.5 การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ไม่เปิดพอร์ตที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องถูกตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

8.6 ผู้ดูแลระบบควรทบทวนสิทธิ์ในการเข้าใช้เครือข่ายภายใน Virtual Private Network (VPN) อย่างน้อย 3 เดือนครั้ง เพื่อให้มั่นใจว่าการเข้าถึงและการใช้งานเครือข่าย VPN ยังคงมีความปลอดภัยและไม่มีการละเมิดสิทธิ์ของผู้ใช้งาน

9. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกสถาบัน

การเข้าสู่ระบบจากระยะไกล (Remote Access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

10. ข้อกำหนดเกี่ยวกับประเภทของข้อมูล และลำดับชั้นความลับของข้อมูล

10.1 ประเภทของข้อมูลหรือรูปแบบของเอกสารอิเล็กทรอนิกส์ กำหนดตามมาตรฐานทั่วไปได้ ดังนี้

10.1.1 รูปแบบเอกสารข้อความ (Text format) ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ เช่น

10.1.1.1 TEXT format เป็นไฟล์ที่เก็บเฉพาะตัวอักษร ไม่เก็บลักษณะที่ใช้

10.1.1.2 Document format เป็นไฟล์ที่ผลิตจาก เวิร์ด โปรเซสเซอร์ เช่น ไมโครซอฟท์เวิร์ด ซึ่งไฟล์ประเภทนี้จะเก็บคุณลักษณะของการแสดงผลของเอกสารไว้พร้อมกับตัวอักษร

10.1.1.3 PDF format (Portable Document Format) เป็นไฟล์เอกสารที่ถูกออกแบบให้สามารถเปิดใช้งานกับระบบคอมพิวเตอร์ต่างระบบกันได้ โดยต้องใช้โปรแกรมในการเปิดและการสร้างเอกสารในรูปแบบ PDF

10.1.1.4 XML (Extensible Markup Language) เป็นภาษาที่ใช้สำหรับการเขียน Markup document โดยมีการใช้ Metadata เพื่อบอกหน้าที่และประเภทของข้อมูลของส่วนต่าง ๆ ในเอกสารนั้น

10.1.2 รูปแบบเอกสารภาพ (Image) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ มีรูปแบบที่ใช้งาน เช่น

10.1.2.1 JPEG format เป็นรูปแบบที่ออกแบบมาเพื่อเก็บภาพได้หลายสี มีการบีบอัดข้อมูล

10.1.2.2 PNG หรือ GIF formats เป็นรูปแบบที่ออกแบบมาเพื่อเก็บภาพ มีการบีบอัดข้อมูลแบบไม่มีการสูญเสียของคุณภาพ

10.1.2.3 Bitmapping formats เป็นรูปแบบที่ออกแบบมาเพื่อเก็บภาพในรูปแบบอื่น ๆ เป็นจุดของภาพ

10.2 การลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.2552 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

10.2.1 การกำหนดชั้นความลับตามความสำคัญของข้อมูล กำหนดไว้ 4 ชั้น ได้แก่ ลับที่สุด ลับมาก ลับ และ ปกปิด และมีการกำหนดความรับผิดชอบให้แก่ผู้มีอำนาจกำหนดชั้นความลับเป็นผู้พิจารณากำหนะระดับชั้นความลับของเอกสาร และการยกเลิก หรือปรับระดับชั้นความลับของเอกสารตามความจำเป็น

10.2.2 การควบคุมเอกสาร กำหนดให้มีมาตรการควบคุมต่าง ๆ คือ การลงทะเบียน การดำเนินการ การส่ง การเก็บรักษา การแจกจ่ายเอกสาร ระดับชั้นการเข้าถึง และการทำลายให้เป็นไปโดยถูกต้อง กรณีที่เป็นหนังสือลับ กำหนดให้ สำนักผู้อำนวยการ เป็นผู้รับผิดชอบในการดำเนินการเกี่ยวกับหนังสือลับเท่านั้น

10.2.3 การเข้ารหัส หรือการถอดรหัสข้อมูลข่าวสารลับ ให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

10.3 การทำลายสื่อบันทึกข้อมูล หรือการทำลายข้อมูลในสื่อชนิดต่าง ๆ ให้ปฏิบัติตามแนวทางดังต่อไปนี้

10.3.1 สื่อบันทึกข้อมูลประเภทกระดาษ ให้ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร

10.3.2 สื่อบันทึกข้อมูลประเภท Flash Drive ให้ใช้วิธีการทุบหรือบดให้เสียเสียหาย

10.3.3 สื่อบันทึกข้อมูลประเภทแผ่น CD/DVD ให้ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร

10.3.4 สื่อบันทึกข้อมูลประเภทฮาร์ดดิสก์ ให้พิจารณาเลือกใช้วิธีการทำลายข้อมูลบนฮาร์ดดิสก์ตามความสำคัญของข้อมูลที่บันทึกหรือจัดเก็บ ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ที่ได้รับการยอมรับ ได้แก่ Fill Sectors With Zero/One, DOD 5220.22 M หรือ NSA เป็นต้น

ส่วนที่ 4
แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอกหรือบุคลากรฝ่ายสนับสนุนอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสถาบันให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบ การใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

2. แนวปฏิบัติทั่วไป

2.1 หัวหน้าสำนักเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศได้

2.2 ในการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานภายนอกหรือบุคลากรฝ่ายสนับสนุนต้องปฏิบัติตามแนวทางดังต่อไปนี้

2.2.1 บุคคลจากหน่วยงานภายนอกหรือบุคลากรฝ่ายสนับสนุนที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสถาบันจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากหัวหน้าสำนักเทคโนโลยีสารสนเทศ

2.2.2 ผู้ขอใช้ระบบต้องกรอกข้อมูลลงใน *“แบบฟอร์มการขออนุญาตเข้าใช้งานระบบสารสนเทศสำหรับหน่วยงานภายนอก”* ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

2.2.2.1 เหตุผลในการขอใช้

2.2.2.2 ระยะเวลาในการใช้

2.2.2.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

2.2.2.4 การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

2.2.2.5 การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูลแล้วจึงยื่นคำขอให้กับเจ้าหน้าที่ผู้รับผิดชอบดำเนินการพิจารณาตามขั้นตอน

2.2.3 หน่วยงานภายนอกที่ทำงานให้กับสถาบันทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในสถาบันหรือนอกสถานที่จำเป็นต้องลงนามใน *“สัญญาการไม่เปิดเผยข้อมูลของสถาบัน”* โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

2.2.4 หลังจากที่ผู้ขอใช้งานระบบจากหน่วยงานภายนอกผ่านการอนุมัติสิทธิเข้าใช้งานระบบแล้ว เจ้าหน้าที่ผู้กำหนดสิทธิการใช้งานระบบจะเป็นผู้กำหนดบัญชีรายชื่อ และรหัสผ่านชั่วคราว โดยระบุลงใน

“แบบฟอร์มกำหนดสิทธิการเข้าใช้ระบบสารสนเทศ” แล้วแจ้งให้ผู้ขอใช้งานระบบจากหน่วยงานภายนอกมารับเอกสารดังกล่าว โดยลงลายมือชื่อรับเอกสาร โดยผู้ขอใช้ต้องเก็บเอกสารดังกล่าวเป็นความลับ และทำการเปลี่ยนแปลงรหัสผ่านเมื่อเข้าใช้งานระบบในครั้งแรก ซึ่งรหัสผ่านที่ผู้ขอใช้งานระบบกำหนดขึ้นมาใหม่ต้องเป็นไปตามแนวปฏิบัติของเอกสาร *“การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”*

2.2.5 สถาบันจะต้องเข้าไปประเมินความเสี่ยงหน่วยงานภายนอก ทั้งนี้ ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศที่เข้าไปปฏิบัติงาน โดยใช้แนวนโยบายตาม *“แนวปฏิบัติในการประเมินความเสี่ยงเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศ” (ส่วนที่ 12)*

2.2.6 เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนามใน *“สัญญาการไม่เปิดเผยข้อมูลของสถาบัน”*

2.2.7 สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของสถาบัน ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

2.2.8 สถาบันมีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้มั่นใจได้ว่าสถาบันสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

2.2.9 ผู้ให้บริการจากหน่วยงานภายนอกจะต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

ส่วนที่ 5
แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

1. วัตถุประสงค์

นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล ผู้ใช้งานจะต้องทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของสถาบันให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

2. แนวปฏิบัติทั่วไป

2.1 เครื่องคอมพิวเตอร์ที่สถาบันอนุญาตให้ผู้ใช้ใช้งาน เป็นทรัพย์สินของสถาบัน ดังนั้น ผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์ของสถาบันอย่างมีประสิทธิภาพเพื่องานของสถาบัน

2.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของสถาบัน ต้องเป็นโปรแกรมที่สถาบันได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.3 ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมใด ๆ ในเครื่องคอมพิวเตอร์ส่วนบุคคลของสถาบัน เว้นแต่ได้รับอนุญาตจากเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศเป็นที่เรียบร้อย

2.4 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ส่วนบุคคลของสถาบันจะต้องกำหนดโดยเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ เท่านั้น

2.5 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลของสถาบันตรวจซ่อมจะต้องได้รับความเห็นและตรวจสอบเบื้องต้นโดยเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศหรือเจ้าหน้าที่พัสดุก่อนเท่านั้น ทั้งนี้ผู้ใช้งาน จะต้องดำเนินการสำรองข้อมูล และลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลก่อนทุกครั้ง

2.6 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

2.7 ไม่เก็บข้อมูลสำคัญของสถาบันไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่ เว้นแต่จัดเก็บไว้บนระบบคลาวด์ Microsoft OneDrive ที่เป็นลิขสิทธิ์ของสถาบัน

2.8 เพื่อรักษาความปลอดภัยของคอมพิวเตอร์จากการใช้งานที่ไม่ถูกต้อง ผู้ใช้งานอาจจะต้องล็อกเครื่องคอมพิวเตอร์ หรือการควบคุมแบบอื่น ๆ เช่น ให้ใส่รหัสผ่าน เมื่อไม่ได้ใช้งาน

2.9 ไม่นำอาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ อยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

2.10 ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์ส่วนบุคคล

3. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

3.1 ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

3.2 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาดให้แจ้งผู้ดูแลระบบทำการแก้ไขทันที

3.3 ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 15 นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

3.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

3.5 ผู้ใช้งานต้องปิดระบบหรือเซสชันที่ใช้งานเสร็จแล้ว ไม่เช่นนั้นก็ต้องใช้กลไกป้องกันการเข้าถึงระบบของระบบปฏิบัติการเป็นตัวล็อค เพื่อไม่ให้ผู้ที่ไม่มีสิทธิใช้งานซึ่งไม่ทราบชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) เข้าใช้งานเครื่องคอมพิวเตอร์

3.6 ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้งานต้อง logout ออกจากเครื่องคอมพิวเตอร์หรือล็อคหน้าจอ หรือได้รับการป้องกันจากการใช้หน้าจอและคีย์บอร์ด หรือการตรวจสอบและยืนยันตัวตนแบบอื่น ที่ไม่ใช่แต่เพียงปิดหน้าจอเท่านั้น

4. แนวปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ใน *“แนวปฏิบัติการบริหารจัดการสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ” (ส่วนที่ 15)* และ *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน” (ส่วนที่ 14)*

5. แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

5.1 ผู้ใช้งานต้องทำการอัพเดท (update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่าง ๆ รวมทั้งโปรแกรมป้องกันไวรัส (Antivirus) อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

5.2 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์

5.3 ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อบันทึกพกพาต่าง ๆ เช่น ฮาร์ดดิสก์แบบติดตั้งภายนอก (External Hard Disk) ธัมบ์ไดรฟ์ (Thumb Drive) ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

5.4 ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

5.5 ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

6. แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

6.1 ผู้ใช้งาน ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น ฮาร์ดดิสก์แบบติดตั้งภายนอก หรือบันทึกไว้บน Microsoft OneDrive เพื่อป้องกันการสูญหายของข้อมูล

6.2 ผู้ใช้งาน ต้องเก็บรักษาสื่อข้อมูลสำรอง (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

6.3 ผู้ใช้งาน ต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บนฮาร์ดดิสก์ประจำเครื่อง ต้องไม่เป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหากฮาร์ดดิสก์เสียไปก็ไม่กระทบต่อการดำเนินการของสถาบัน

6.4 แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

ส่วนที่ 6
แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์แบบพกพา

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกสถาบัน รวมทั้งเป็นมาตรการป้องกันข้อมูลและอุปกรณ์ของสถาบันให้เกิดความปลอดภัย ผู้ใช้งานจะต้องรับทราบถึงข้อกำหนดและแนวปฏิบัติในการใช้งาน การบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยง เพื่อให้ผู้ใช้งานสามารถใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

2. แนวปฏิบัติทั่วไป

2.1 เครื่องคอมพิวเตอร์แบบพกพาที่สถาบันอนุญาตให้ผู้ใช้ใช้งาน เป็นทรัพย์สินของสถาบัน ดังนั้น ผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาของสถาบันอย่างมีประสิทธิภาพเพื่องานของสถาบัน

2.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของสถาบัน ต้องเป็นโปรแกรมที่สถาบันได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.3 ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมใด ๆ ในเครื่องคอมพิวเตอร์แบบพกพาของสถาบัน

2.4 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) แบบพกพาของสถาบันจะต้องกำหนดโดยเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ เท่านั้น

2.5 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาของสถาบันตรวจซ่อมจะต้องได้รับความเห็นและตรวจสอบเบื้องต้นโดยเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศก่อน เท่านั้น ทั้งนี้ผู้ใช้งาน จะต้องดำเนินการสำรองข้อมูล และลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลก่อนทุกครั้ง

2.6 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

2.7 ไม่เก็บข้อมูลสำคัญของสถาบันไว้บนเครื่องคอมพิวเตอร์แบบพกพาที่ท่านใช้งานอยู่ เว้นแต่จัดเก็บบนระบบคลาวด์ Microsoft OneDrive ที่เป็นลิขสิทธิ์ของสถาบัน

2.8 เพื่อรักษาความปลอดภัยของคอมพิวเตอร์จากการใช้งานที่ไม่ถูกต้อง ผู้ใช้งานอาจจะใช้กุญแจล็อกหรือการควบคุมแบบอื่น ๆ เช่น ให้ใส่รหัสผ่าน เมื่อไม่ได้ใช้งาน

2.9 ผู้ใช้งาน ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

2.10 ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

2.11 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

2.12 ไม่ใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

2.13 การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

2.14 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

2.15 ไม่วางของทับบนหน้าจอและแป้นพิมพ์

2.16 ไม่เคลื่อนย้ายเครื่องในขณะที่ฮาร์ดดิสก์กำลังทำงาน

2.17 ไม่ใช้ หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ หรือเครื่องดื่มต่าง ๆ เป็นต้น

2.18 ไม่ใช้ หรือวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

2.19 ไม่ติดตั้ง หรือวางคอมพิวเตอร์แบบพกพาในที่ที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่

3. แนวปฏิบัติด้านความปลอดภัยทางกายภาพ

3.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ต้องล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

3.2 ผู้ใช้งานต้องไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

3.3 ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่

4. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

4.1 ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

4.2 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาดให้แจ้งผู้ดูแลระบบทำการแก้ไขทันที

4.3 ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen saver) โดยตั้งเวลาประมาณ 15 นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

4.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

4.5 ผู้ใช้งานต้องปิดระบบหรือเซสชั่นที่ใช้งานเสร็จแล้ว ไม่เช่นนั้นก็ต้องใช้กลไกป้องกันการเข้าถึงระบบของระบบปฏิบัติการเป็นตัวล็อค เพื่อไม่ให้ผู้ที่ไม่มีสิทธิใช้งานซึ่งไม่ทราบชื่อผู้ใช้งาน (User name) และรหัสผ่าน (Password) เข้าใช้งานเครื่องคอมพิวเตอร์

4.6 ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้งานต้อง logout ออกจากเครื่องคอมพิวเตอร์ หรือล็อคหน้าจอด้วยโปรแกรม Screen saver หรือได้รับการป้องกันจากการใช้หน้าจอและคีย์บอร์ด หรือการป้องกันโดยใช้รหัสผ่านอุปกรณ์ Token หรือการตรวจสอบและยืนยันตัวตนแบบอื่น ที่ไม่ใช่แต่เพียงปิดหน้าจอเท่านั้น

5. แนวปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้งานปฏิบัติตาม แนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ใน *“แนวปฏิบัติการบริหารจัดการสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ” (ส่วนที่ 15)* และ *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน” (ส่วนที่ 14)*

6. แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

6.1 ผู้ใช้งานต้องทำการอัพเดท (Update) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมใช้งานต่าง ๆ รวมทั้งโปรแกรมป้องกันไวรัส (Antivirus) อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

6.2 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์

6.3 ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อบันทึกพกพาต่าง ๆ เช่น ฮาร์ดดิสก์แบบติดตั้งภายนอก (External Hard disk) ธัมบ์ไดรฟ์ (Thumb drive) ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

6.4 ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

6.5 ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

6.6 หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

7. แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

7.1 ผู้ใช้งาน ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาไว้บนสื่อบันทึกอื่น ๆ เช่น ระบบคลาวด์ Microsoft OneDrive หรือ ฮาร์ดดิสก์แบบติดตั้งภายนอก เพื่อป้องกันการสูญหายของข้อมูล

7.2 ผู้ใช้งาน ต้องเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

7.3 ผู้ใช้งาน ต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บนฮาร์ดดิสก์ประจำเครื่อง ต้องไม่เป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหากฮาร์ดดิสก์เสียไปก็ไม่กระทบต่อการดำเนินการของสถาบัน

7.4 แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

ส่วนที่ 7
แนวปฏิบัติการใช้งานอินเทอร์เน็ต

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของสถาบันถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

2.1 ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่สถาบันจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เครือข่ายอินเทอร์เน็ตไร้สายของสถาบัน เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Wireless Router ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรแล้ว

2.2 ก่อนที่จะนำเครื่องคอมพิวเตอร์ส่วนบุคคลเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ เว็บเบราเซอร์

2.3 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต ผู้ใช้งานต้องทำการทดสอบไวรัส (Virus scanning) โดยใช้โปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง และควรหมั่นตรวจสอบการ Update ระบบปฏิบัติการและการตั้งค่าเบราว์เซอร์อุปกรณ์ต่างให้ทันสมัยอยู่เสมอ

2.4 ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของสถาบันเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่มีความเสี่ยงที่จะก่อให้เกิดปัญหาทางความมั่นคงปลอดภัยแก่ผู้ใช้งาน เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

2.5 ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของสถาบัน

2.6 ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับสถาบัน

2.7 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสถาบันที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

2.8 ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

2.9 ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

2.10 ผู้ใช้งานต้องมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

2.11 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

2.12 ในการใช้งานโซเชียลมีเดีย (Social Media) ของสถาบัน ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสถาบัน

2.13 ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสถาบัน การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

2.14 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ส่วนที่ 8
แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์

1. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของสถาบัน ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวปฏิบัติทั่วไป

2.1 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของสถาบัน ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

2.2 สำนักทรัพยากรบุคคล จะจัดส่งรายชื่อเจ้าหน้าที่ใหม่ให้กับสำนักเทคโนโลยีสารสนเทศเพื่อดำเนินการกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน

2.3 ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของสถาบัน

2.4 ผู้ใช้งานต้องกำหนดรหัสผ่านที่ดี (Good Password) ตามแนวปฏิบัติที่ระบุไว้ใน *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน” (ส่วนที่ 14)*

2.5 ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ ซึ่งในทางปฏิบัติโดยทั่วไปไม่ควรเกิน 3 ครั้ง

2.6 ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ควรมีการ logout ออกจากหน้าจอตัดการใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

2.7 ผู้ใช้งานไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) ของระบบจดหมายอิเล็กทรอนิกส์

2.8 ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 6 เดือน เป็นตามความสมัครใจไม่บังคับเปลี่ยน โดยขอให้ผู้ใช้งานกำหนดรหัสผ่านที่มั่นคง รัดกุม และปลอดภัย สอดคล้องตาม *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน” (ส่วนที่ 14)*

2.9 ผู้ใช้งานควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อสถาบัน หรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์

หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของสถาบัน

2.10 ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่น เพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

2.11 ผู้ใช้งานควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของสถาบัน เพื่อการทำงานของสถาบันเท่านั้น การให้บริการจดหมายอิเล็กทรอนิกส์ของสถาบัน สงวนสิทธิให้ผู้ใช้งาน ใช้เพื่อติดต่อสื่อสารทั่วไป ห้ามนำไปใช้ในเชิงการค้าเพื่อประโยชน์ส่วนบุคคล

2.12 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานควรทำการ logout ออกจากระบบทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

2.13 ผู้ใช้งานควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

2.14 ผู้ใช้งานไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

2.15 ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของสถาบัน ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

2.16 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

2.17 ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

2.18 ผู้ใช้งานควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

2.19 ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตนเพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้น ไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในกล่องจดหมายอิเล็กทรอนิกส์

2.20 ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ ควรให้ความรู้เกี่ยวกับการรักษาความปลอดภัยในจดหมายอิเล็กทรอนิกส์แก่ผู้ใช้งานจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอ การให้ความรู้ถือเป็นการป้องกันเบื้องต้นเพื่อมิให้ผู้ใช้งานตกเป็นเหยื่อของผู้ไม่หวังดี และเป็นการป้องกันไม่ให้เกิดปัญหาในกรณีที่ทำผิดพลาดแม้เพียงครั้งเดียว อาจส่งผลกระทบทำให้ระบบไม่สามารถทำงานได้

2.21 ในการใช้จดหมายอิเล็กทรอนิกส์ในการติดต่อสื่อสารนั้น ผู้ใช้งานควรให้เกียรติกับผู้รับปลายทางเหมือนการสนทนาด้วยวาจา ควรตรวจสอบตัวสะกดไวยากรณ์ อ่านทวนเนื้อหาก่อนส่ง ใช้ข้อความที่กระชับเข้าถึงประเด็นอย่างรวดเร็ว แต่ข้อความต้องไม่สั้นเกินจนดูแล้วห้วน และให้ตระหนักอยู่เสมอว่าข้อความใด ๆ

ที่ส่งผ่านเครือข่ายอินเทอร์เน็ตนั้นเป็นข้อความที่สามารถมองเห็น และอ่านได้โดยผู้อื่น ดังนั้น การส่งข้อความที่เป็นความลับจะต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อเข้ารหัสข้อมูลนั้นก่อนส่งออกไป

2.22 ผู้ใช้งานต้องไม่ทำการเปลี่ยนแปลง หรือแก้ไขข้อความจดหมายอิเล็กทรอนิกส์ต้นฉบับที่ได้รับมาและต้องการส่งต่อไป หากจดหมายอิเล็กทรอนิกส์นั้นถูกส่งถึงผู้รับเป็นการส่วนตัว ต้องขออนุญาตผู้ส่งก่อนที่จะส่งต่อจดหมายอิเล็กทรอนิกส์นั้นไปจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลส่วนบุคคล ควรได้รับการเข้ารหัสอย่างปลอดภัย (Encryption)

2.23 ผู้ใช้งานควรใส่ชื่อหัวข้อเรื่องใน Subject ของจดหมายอิเล็กทรอนิกส์ เพื่อแสดงถึงเรื่องของจดหมายอิเล็กทรอนิกส์ที่ต้องการหารือหรือแจ้งให้ทราบ และควรส่งจดหมายอิเล็กทรอนิกส์ตอบกลับสั้น ๆ หากไม่มีเวลาพอเพื่อให้ผู้ส่งได้รับทราบว่าผู้รับได้รับจดหมายอิเล็กทรอนิกส์นั้นแล้ว และจะตอบกลับอย่างสมบูรณ์ในภายหลัง

2.24 ผู้ใช้งานต้องไม่ส่งต่อจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งที่ไม่สมควรทำบนเครือข่ายอินเทอร์เน็ต จดหมายชี้ชวน หรือ อื่น ๆ อันเป็นการกระทำที่เข้าข่าย spam หรือ unsolicited electronic mail อย่างเด็ดขาด หากได้รับจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ และมีข้อความขอให้ส่งต่อจดหมายอิเล็กทรอนิกส์นั้นให้ติดต่อหรือแจ้งผู้ดูแลระบบโดยทันที

2.25 ผู้ใช้งานไม่ควรส่งจดหมายอิเล็กทรอนิกส์ที่เกี่ยวกับการล่วงละเมิดหรือข่มขู่ หรือมีเนื้อหาข้อความที่ขัดต่อกฎหมายและศีลธรรม และใช้จดหมายอิเล็กทรอนิกส์เป็นเครื่องมือในการกระจายข่าวสาร เว้นแต่เป็นการประกาศที่เหมาะสม

2.26 ผู้ใช้งานควรพิจารณาใช้ “BCC” (Blind Carbon Copy – สำเนาโดยที่ผู้รับไม่ทราบ) ในการส่งจดหมายอิเล็กทรอนิกส์ถึงผู้รับเป็นจำนวนมาก เพื่อไม่ให้รายชื่อผู้รับทั้งหมดปรากฏในลักษณะที่ยาวมากเกินไป

2.27 ผู้ใช้งานควรทำตามนโยบายอย่างเคร่งครัด และแจ้งผู้ดูแลระบบเมื่อพบการใช้จดหมายอิเล็กทรอนิกส์ที่ไม่ถูกต้อง

2.28 ผู้ใช้งานต้องกรอกข้อมูลในช่องข้อมูลส่วนตัว (Identity) โดยจะต้องใช้ชื่อผู้ส่ง (Sender) ที่เป็นจริงตามที่มีบัญชีรายชื่ออยู่จริง เพื่อให้สามารถอ้างอิงในกรณีที่มีปัญหาเกิดขึ้น

2.29 ผู้ใช้งานต้องไม่ตั้งชื่อผู้ส่ง (Sender) หรือข้อมูลอื่น ในลักษณะที่ส่อว่าเป็นผู้ดูแลระบบ (Administrator) เช่น webmaster, host master, administrator, admin, postmaster เป็นต้น โดยไม่ได้รับอนุญาต

2.30 ผู้ใช้บริการมีหน้าที่จะต้องรักษาชื่อผู้ใช้งาน และรหัสผ่านเป็นความลับ ไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

2.31 จดหมายของผู้ใช้บริการ ถือเป็นข้อมูลส่วนบุคคล ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ไม่สามารถจะทำการเก็บ กู้ หรือดึงข้อมูลส่วนตัวขึ้นมาได้ ดังนั้น ผู้ใช้บริการจะต้องดูแลรักษาข้อมูลดังกล่าวอย่างระมัดระวัง โดยเฉพาะการลบจดหมายที่ไม่ต้องการ รวมทั้งจะต้องดูแลรักษาไม่ให้ขนาดของจดหมายที่จัดเก็บเกินกว่าจำนวนพื้นที่ที่ได้รับอนุญาต

2.32 ผู้ใช้งานต้องมีความรับผิดชอบ และระมัดระวังในการใช้บริการตามสมควร ไม่ให้ล่วงละเมิดบุคคลอื่น รวมถึงศีลธรรม หรือกฎหมายใด ๆ อันเป็นผลให้เกิดความไม่สงบเรียบร้อยในสถาบันและสังคม

2.33 ในกรณีที่ทางสำนักเทคโนโลยีสารสนเทศ ตรวจพบว่า ผู้ใช้งานได้ละเมิดข้อกำหนดการใช้งานระบบจดหมายอิเล็กทรอนิกส์ จะทำการระงับการให้บริการและทำการตรวจสอบทันที เพื่อเป็นการรักษาผลประโยชน์ของผู้ใช้บริการโดยส่วนรวม และของสถาบัน อีกทั้งในกรณีที่การละเมิดดังกล่าว เป็นการกระทำอันขัดต่อกฎหมายจะต้องได้รับโทษตามที่ระบุไว้ ทั้งนี้ การใช้งานระบบจดหมายอิเล็กทรอนิกส์ของทางสำนักเทคโนโลยีสารสนเทศ จะถือว่าผู้ที่ใช้ ได้รับทราบ ทำความเข้าใจ และได้ยอมรับข้อกำหนดตามที่ระบุในฉบับนี้แล้ว

2.34 กรณีเจ้าหน้าที่ลาออก ให้สำนักทรัพยากรบุคคลแจ้งให้สำนักเทคโนโลยีสารสนเทศทราบ และผู้ดูแลระบบต้องทำการลบบัญชีผู้ใช้งาน ภายใน 3 วันทำการ

ส่วนที่ 9
แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของสถาบัน โดยการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. แนวปฏิบัติ

2.1 บทบาทหน้าที่ของผู้ดูแลระบบ

2.1.1 ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.1.2 ผู้ดูแลระบบจะต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

2.1.3 ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

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

2.1.5 ผู้ดูแลระบบควรเปลี่ยนค่าชื่อ login และรหัสผ่าน สำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อ login และรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

2.1.6 ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ Access Point เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

2.1.7 ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC address และชื่อผู้ใช้ (User name) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address และชื่อผู้ใช้รหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

2.1.8 ผู้ดูแลระบบควรจะมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในสถาบัน

2.1.9 ผู้ดูแลระบบควรกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับช่องสัญญาณ SSID (Service Set Identifier) ที่กำหนดไว้เท่านั้น เพื่อช่วยป้องกันการโจมตี

2.1.10 ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

2.1.11 ผู้ดูแลระบบควรทบทวนชื่อบัญชีผู้ใช้งานในระบบเพื่อป้องกันการใช้งานเครือข่ายไร้สายที่ไม่ได้รับอนุญาต

2.2 ผู้ใช้งานทั้งที่เป็นผู้ปฏิบัติงานสถาบันและไม่ใช่ผู้ปฏิบัติงาน ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของสถาบัน ต้องมีการยืนยันตัวตนตามระบบที่สถาบันกำหนด

ส่วนที่ 10
แนวปฏิบัติในการสำรองข้อมูล

1. วัตถุประสงค์

เพื่อให้ระบบสารสนเทศของสถาบันสามารถดำเนินการได้อย่างต่อเนื่อง ข้อมูลไม่สูญหาย ในกรณีที่เกิดความเสียหายต่ออุปกรณ์คอมพิวเตอร์ และเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งเป็นที่จัดเก็บข้อมูลงานสำคัญและระบบฐานข้อมูล

2. ระบบสารสนเทศที่มีความจำเป็นในการสำรองข้อมูล

ระบบสารสนเทศทุกระบบ จะต้องมีการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้องครบถ้วน ทั้ง ระบบซอฟต์แวร์ และข้อมูลในทุกระบบข้อมูล แยกตามระบบสารสนเทศแต่ละระบบ ซึ่งมีขั้นตอนปฏิบัติดังต่อไปนี้

2.1 ระบบซอฟต์แวร์ จะทำการสำรองข้อมูลทุกครั้งที่มีการแก้ไขหรือปรับปรุงระบบ หรืออย่างน้อยเดือนละ 1 ครั้ง

2.2 ระบบข้อมูล จะทำการสำรองข้อมูลทุกวัน โดยเลือกช่วงเวลาที่มีการใช้งานน้อยที่สุดหรือไม่มีการใช้งานเพื่อไม่ให้กระทบต่อการทำงานของผู้ใช้งาน

2.3 การสำรองข้อมูล จะทำการสำรองแบบ Full Backup และไม่ควรจัดเก็บไว้ในที่เดียวกับระบบข้อมูล

2.4 การสำรองข้อมูลทุกครั้งจะต้องทำการตรวจสอบความถูกต้องของข้อมูลที่ทำการสำรอง

2.5 ระบบซอฟต์แวร์และข้อมูลที่ทำการสำรอง จะถูกรวบรวมเพื่อนำไปเก็บรักษาไว้ที่ *“สถานที่เก็บข้อมูลสำรอง”* เป็นประจำทุกเดือน

3. รูปแบบข้อมูลที่สำรอง

ข้อมูลที่สำรองในแต่ละระบบตามขั้นตอนที่กำหนดไว้ข้างต้นแล้ว แปลงให้อยู่ในรูปแบบบีบอัดข้อมูลเป็นแฟ้มข้อมูลเดียวของแต่ละระบบโดยใช้มาตรฐานการบีบอัดข้อมูลแบบ ZIP และอาจจะมีการตรวจสอบความถูกต้องของข้อมูลเพื่อสร้างความเชื่อมั่นในความถูกต้องของข้อมูล ซึ่งอาจจะมีการสร้างลายมือชื่ออิเล็กทรอนิกส์โดยใช้มาตรฐาน XML Signature และเพื่อรักษาความลับของข้อมูลนั้นให้มีการเข้ารหัสโดยใช้รูปแบบข้อมูล XML Encryption

4. สถานที่เก็บข้อมูลสำรอง

การเก็บข้อมูลที่สำรองนั้นต้องถูกจัดเก็บในสื่อเก็บข้อมูลแบบฮาร์ดดิสพกพา (External HDD) ระบบคลาวด์ (Cloud) Microsoft OneDrive โดยมีการกำหนดชื่อโฟลเดอร์อย่างชัดเจน สามารถแสดงถึงระบบซอฟต์แวร์และวันที่เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลได้อย่างชัดเจนเพื่อให้รู้ได้ว่าเป็นข้อมูลสำรองของระบบสารสนเทศใดและทำสำรองเมื่อใด โดยใคร ข้อมูลสำรองควรจัดเก็บไว้ที่หน่วยงานอื่น หรือระบบคลาวด์ (Cloud)

5. การทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

มีการทดสอบสื่อเก็บข้อมูล ฮาร์ดดิสพกพา (External HDD), ระบบคลาวด์ (Cloud), Microsoft OneDrive อย่างสม่ำเสมอทุกระบบ อย่างน้อยเดือนละ 1 ครั้ง

ส่วนที่ 11
แนวปฏิบัติในการสร้างความต่อเนื่องให้กับธุรกิจ

1. คำนำ

กระบวนการสร้างความต่อเนื่องให้กับธุรกิจในที่นี้ หมายถึง การบริหารจัดการเพื่อให้สถาบันดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารได้อย่างต่อเนื่อง แม้ในช่วงสภาวะที่เกิดปัญหาหรือเหตุการณ์ผิดปกติอันเนื่องมาจากความล้มเหลวของระบบเครือข่าย ระบบฐานข้อมูล ภัยพิบัติทางธรรมชาติ อุบัติเหตุ ความบกพร่องของเครื่องมืออุปกรณ์ รวมทั้งการกระทำผิดส่วนบุคคลในกรณีประมาทเลินเล่อหรือกระทำอย่างตั้งใจก็ตาม ทั้งนี้ เพื่อลดผลกระทบที่มีต่อสถาบันไม่ให้ภารกิจต้องหยุดชะงักเป็นเวลานาน เปลี่ยนเป็นชะลอการทำงานในระดับที่ยอมรับได้

นอกจากนี้ยังจะต้องสร้างความเชื่อมั่นให้แก่ทุกฝ่ายในการกู้คืนทรัพยากรของระบบสารสนเทศให้สามารถนำกลับมาใช้งานได้ตามปกติ หรือใกล้เคียงสภาพปกติได้มากที่สุดในระดับที่ทุกฝ่ายยอมรับได้ ด้วยการดูแลการปฏิบัติของเจ้าหน้าที่ เครื่องมืออุปกรณ์ ระบบซอฟต์แวร์ และทรัพยากรที่เกี่ยวข้อง ให้มีความพร้อมรองรับการใช้งานได้อย่างต่อเนื่อง โดยผ่านการดำเนินงานตามแนวปฏิบัติในแผนงานและการประเมินความเสี่ยงที่มีผลต่อการหยุดชะงักของการปฏิบัติภารกิจ ดังนี้

2. แนวปฏิบัติในกระบวนการในการสร้างความต่อเนื่องให้กับธุรกิจ

2.1 จัดประชุมชี้แจงเพื่อสร้างความเข้าในประเด็นความเสี่ยงที่สถาบันอาจต้องประสบ โดยประกอบด้วย

2.1.1 ระบุความเสี่ยง และจัดลำดับความสำคัญของภารกิจที่เกี่ยวข้อง

2.1.2 ระบุทรัพยากรสารสนเทศ ทั้งเครื่องมืออุปกรณ์และฐานข้อมูล ในกระบวนการที่เป็นภารกิจสำคัญ

2.1.3 ผลกระทบที่มีต่อการปฏิบัติภารกิจในภาวะความเสี่ยงและแนวทางจัดการ โดยกำหนดวัตถุประสงค์ของการจัดการความเสี่ยงดังกล่าว

2.2 จัดสรรงบประมาณสำหรับดำเนินการในส่วนที่เกี่ยวข้องกับทรัพยากร โครงสร้างการบริหารงานด้านเทคโนโลยี และสิ่งแวดล้อม รวมทั้งเริ่มดำเนินการทันทีเพื่อป้องกันหรือผ่อนคลายผลกระทบจากความเสี่ยงดังกล่าว

2.3 จัดทำเอกสารแผนการทำงานในภาวะฉุกเฉินหรือเกิดเหตุการณ์ผิดปกติ เพื่อสร้างความต่อเนื่องของการดำเนินงานตามภารกิจของแต่ละฝ่าย

2.4 จัดให้มีการทดสอบและปรับปรุงกระบวนการสร้างความต่อเนื่องให้กับธุรกิจอย่างสม่ำเสมอ

2.5 จัดให้มีโครงสร้างการบริหารและบุคลากรผู้รับผิดชอบต่อกระบวนการสร้างความต่อเนื่องให้กับธุรกิจในแต่ละขั้นตอน

3. แนวปฏิบัติในการประเมินความเสี่ยงในการสร้างความต่อเนื่องให้กับธุรกิจ

3.1 ระบุเหตุการณ์ซึ่งเป็นต้นเหตุของการหยุดชะงักในการปฏิบัติภารกิจ ความน่าจะเป็นหรือโอกาสที่จะเกิดเหตุการณ์ดังกล่าว รวมทั้งผลกระทบที่เกิดขึ้นทันทีและที่จะเกิดตามมาในภายหลัง

3.2 ระบุสาเหตุที่อาจทำให้เกิดความล้มเหลวของเครื่องมืออุปกรณ์ ความผิดพลาดของบุคลากร การโจรกรรมข้อมูล และการก่ออาชญากรรมทางคอมพิวเตอร์

3.3 จัดให้มีการประเมินความเสี่ยง เพื่อที่จะกำหนดความน่าจะเป็นและความรุนแรงของผลกระทบที่เกิดขึ้น อย่างน้อยปีละ 1 ครั้ง

3.4 พิจารณาภารกิจให้ครอบคลุมทุกกระบวนการ ไม่จำกัดเฉพาะระบบข้อมูล เพื่อที่จะได้มองเห็นผลกระทบที่เกิดขึ้นในภาพรวมทั้งหมดของสถาบัน

3.5 การประเมินความเสี่ยง ให้จัดลำดับความสำคัญของความเสี่ยงเป็นตัวเลข โดยคำนึงถึงความร้ายแรงและผลกระทบต่อภารกิจ ซึ่งครอบคลุมถึงทรัพยากรสารสนเทศ ผลกระทบต่อการหยุดชะงักของการปฏิบัติภารกิจ ระยะเวลาหยุดชะงักที่ยอมรับได้ และการกู้คืนข้อมูลตามลำดับความสำคัญ

3.6 กำหนดให้มีแนวทาง วิธีการ หรือกลยุทธ์ในการดำเนินการ เพื่อรักษาความต่อเนื่องบนพื้นฐานจากผลของการประเมินความเสี่ยง

3.7 เผยแพร่ให้มีการรับรู้และอนุญาตให้ดำเนินการอย่างเป็นทางการ ตามข้อกำหนดแนวทาง วิธีการหรือกลยุทธ์ที่กำหนดไว้

4. แนวปฏิบัติในการจัดทำและใช้งานแผนสร้างความต่อเนื่องให้กับธุรกิจ

4.1 จัดให้มีการทำแผนและดำเนินการตามแผน โดยคำนึงถึงภารกิจของหน่วยงานเป็นสำคัญ เพื่อรักษาความต่อเนื่องของการปฏิบัติงาน และสร้างความเชื่อมั่นในความพร้อมใช้งานได้อย่างต่อเนื่องของระบบข้อมูลในระดับที่ยอมรับได้

4.2 กำหนดหน้าที่ความรับผิดชอบและการยินยอมดำเนินการตามขั้นตอนในการรักษาความต่อเนื่องของการปฏิบัติภารกิจที่กำหนดขึ้น

4.3 ระบุการยอมรับความสูญเสียของข้อมูลและบริการ ที่อาจเกิดขึ้นจากเหตุการณ์ที่ก่อให้เกิดการหยุดชะงักของการปฏิบัติภารกิจ

4.4 ดำเนินการตามขั้นตอนที่กำหนด เพื่อรักษาความต่อเนื่องของการปฏิบัติภารกิจ โดยให้ความสำคัญกับผลกระทบที่ต่อเนื่องกับหน่วยภารกิจอื่น ทั้งภายในและภายนอกที่เกิดจากเหตุการณ์

4.5 กำหนดขั้นตอนปฏิบัติงานสำหรับการกู้คืนงานที่ยังอยู่ระหว่างการดำเนินการก่อนที่ระบบข้อมูลจะหยุดชะงักไป

4.6 จัดให้มีการจัดทำกระบวนการและขั้นตอนปฏิบัติเป็นเอกสาร รวมทั้งจัดฝึกอบรมบุคลากรที่เกี่ยวข้องในกระบวนการและขั้นตอนปฏิบัติที่ได้รับการอนุมัติแล้ว

4.7 ระบุทรัพยากรและสิ่งที่จำเป็นในการดำเนินการให้ชัดเจน รวมทั้งด้านทรัพยากรบุคคลและทรัพยากรที่ไม่ใช่สารสนเทศ

4.8 ในบางขั้นตอนกระบวนการอาจมีหน่วยงานอื่นเข้าร่วมเป็นส่วนหนึ่งด้วยก็ได้ ไม่จำเป็นต้องเป็นหน่วยงานเดียวกันทั้งหมด

4.9 ให้มีการจัดทำสำเนาแผน และเก็บรักษาไว้ในสถานที่อื่นซึ่งห่างไกลเพียงพอที่จะไม่ได้รับผลกระทบจากความเสียหายที่เกิดจากเหตุการณ์ที่ระบุไว้

4.10 สิ่งอื่น ๆ นอกจากแผนแล้ว ถ้าสิ่งนั้นจำเป็นต้องใช้ในการปฏิบัติตามแผน ให้จัดเก็บไว้ในสถานที่นั้นเช่นกัน

4.11 กรณีที่มีการใช้สถานที่อื่นที่เป็นสถานที่ทำการชั่วคราว การจัดทำแผนและการดำเนินงานต้องอยู่ในระดับเดียวกันกับสถานที่ทำการหลัก

4.12 จัดให้มีการทดสอบและปรับปรุงแผนอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าแผนรักษาความต่อเนื่องนั้นถูกต้อง เป็นปัจจุบัน

5. แนวปฏิบัติในการกำหนดกรอบสำหรับการวางแผนเพื่อสร้างความต่อเนื่องให้กับธุรกิจ

5.1 กรอบแนวปฏิบัติเพื่อการรักษาความต่อเนื่องของภารกิจจะต้องได้รับการดูแลบำรุงรักษาและสร้างความเชื่อมั่นได้ว่าแผนดำเนินการต่าง ๆ มีความสอดคล้องกับความต้องการของหน่วยงานเพื่อที่จะสามารถจัดลำดับความสำคัญในการฝึกซ้อมหรือดูแลรักษาได้

5.2 แผนการรักษาความต่อเนื่องทุกแผน จะต้องอธิบายหลักการและวิธีการที่นำมาประยุกต์ใช้

5.3 แต่ละแผนให้มีการกำหนดแผนเพิ่มเติมหรือแผนสำรอง รวมทั้งเงื่อนไขในการเลือกใช้แผน พร้อมทั้งระบุผู้รับผิดชอบดำเนินการในแต่ละส่วน

5.4 เมื่อมีการระบุความต้องการใหม่หรือความจำเป็นใหม่เพิ่มเติมขึ้นมา ขั้นตอนปฏิบัติยามฉุกเฉินเดิมต้องได้รับการแก้ไขอย่างเหมาะสมด้วย

5.5 ขั้นตอนปฏิบัติเหล่านี้ให้บรรจุไว้เป็นส่วนหนึ่งของการบริหารการเปลี่ยนแปลงของสถาบันด้วย เพื่อที่จะสร้างความเชื่อมั่นได้ว่าการรักษาความต่อเนื่องนี้จะได้รับการปฏิบัติ

5.6 ให้มีการกำหนดเจ้าของแผนหรือผู้รับผิดชอบโดยเฉพาะของแต่ละแผนด้วย

5.7 ขั้นตอนปฏิบัติกรณีฉุกเฉิน แผนการกู้คืน ให้อยู่ภายใต้ความรับผิดชอบของบุคลากรผู้ที่เป็นเจ้าของทรัพยากรสารสนเทศที่เกี่ยวข้องนั้น

5.8 การกู้คืนโดยใช้ผู้ให้บริการรายอื่น (ที่ไม่ใช่รายเดิม) เช่น ระบบประมวลผลข้อมูล หรือระบบเครือข่ายคอมพิวเตอร์ เป็นต้น ให้ถือเป็นความรับผิดชอบของผู้ให้บริการปัจจุบัน

5.9 กำหนดเงื่อนไขสำหรับการตัดสินใจใช้แผนปฏิบัติการก่อนที่จะอนุมัติแผนนั้น

5.10 ขั้นตอนกรณีฉุกเฉิน จะต้องอธิบายถึงกิจกรรมที่ต้องดำเนินการสำหรับแต่ละเหตุการณ์

5.11 ขั้นตอนปฏิบัติในการกู้คืน จะต้องอธิบายกิจกรรมที่จำเป็นในการเคลื่อนย้ายไปยังสถานที่ชั่วคราว และการเคลื่อนย้ายกลับคืนมาได้ภายในระยะเวลาที่ยอมรับได้

5.12 ขั้นตอนปฏิบัติชั่วคราวสำหรับการสานต่องานที่ยังคั่งค้างอยู่

5.13 ขั้นตอนปฏิบัติสำหรับการกู้คืนสู่สภาพเดิม ซึ่งอธิบายกิจกรรมที่ต้องดำเนินการ

5.14 กำหนดการสำหรับการทดสอบหรือฝึกซ้อมการดำเนินการตามแผน

5.15 จัดให้มีกิจกรรมในการสร้างความตระหนัก และฝึกอบรม ให้บุคลากรมีความเข้าใจในกระบวนการรักษาความต่อเนื่องของภารกิจ เพื่อให้มั่นใจได้ว่าจะสามารถดำเนินการได้เมื่อมีเหตุการณ์เกิดขึ้นจริง

5.16 กำหนดบทบาทหน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับกิจกรรมในแผน

5.17 กำหนดหรือระบุเครื่องมืออุปกรณ์และทรัพยากรที่จำเป็นต้องใช้ในการปฏิบัติตามแผน

6. แนวปฏิบัติในการทดสอบและการปรับปรุงแผนสร้างความต่อเนื่องให้กับธุรกิจ

6.1 แผนการรักษาความต่อเนื่องในการปฏิบัติงาน จะต้องได้รับการทดสอบ ซักซ้อม ทบทวน และปรับปรุงอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าสามารถใช้งานได้จริง และบุคลากรที่เกี่ยวข้องสามารถที่จะเข้าใจแผนและบทบาทของแต่ละหน่วยงานได้เป็นอย่างดี

6.2 การซ้อมสามารถทำได้บนพื้นฐานของเหตุการณ์สมมติ

6.3 การซ้อมสามารถทำได้โดยใช้วิธีการจำลองสถานการณ์ขึ้น

6.4 จัดให้มีการทดสอบการซ้อมกู้ข้อมูลคืนจริง

6.5 จัดให้มีการทดสอบซ้อมกู้ข้อมูลคืน ณ สถานที่ชั่วคราวที่เตรียมไว้สำรอง

6.6 จัดให้มีการทดสอบร่วมกับหน่วยงานอื่นที่เกี่ยวข้อง

6.7 จัดให้มีการซ้อมแบบสมบูรณ์เต็มรูปแบบด้วย

6.8 เทคนิควิธีการในการทดสอบและซ้อมดำเนินการเหล่านี้สามารถนำไปใช้ได้ขึ้นอยู่กับความจำเป็นและความต้องการ

6.9 ผลการทดสอบหรือซ้อม จะต้องได้รับการบันทึกอย่างเป็นระบบเพื่อการปรับปรุงแก้ไขในอนาคต

6.10 จัดให้มีผู้รับผิดชอบในการทบทวนแผนการรักษาความต่อเนื่องในการปฏิบัติงาน และจะต้องดำเนินการอย่างน้อยปีละ 1 ครั้ง

6.11 การเปลี่ยนแปลงที่เกิดขึ้นกับกระบวนการปฏิบัติงานปกติ จะได้รับการสะท้อนในการปรับปรุงแผนการรักษาความต่อเนื่องด้วย

6.12 การเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้น จะได้รับการควบคุมอย่างเป็นระบบและอย่างเป็นทางการ เพื่อให้เชื่อมั่นได้ว่าแผนล่าสุดที่ถูกต้องจะถึงมือผู้เกี่ยวข้อง

6.13 การเปลี่ยนแปลงที่จะต้องพิจารณาเพื่อการควบคุมอย่างเป็นระบบและเป็นทางการ ประกอบด้วย

6.13.1 การเปลี่ยนแปลงบุคลากร

6.13.2 การเปลี่ยนแปลงที่อยู่และหมายเลขโทรศัพท์

6.13.3 การเปลี่ยนแปลงวิธีการปฏิบัติงาน

6.13.4 การเปลี่ยนแปลงสถานที่ อุปกรณ์ และทรัพยากรอื่น ๆ

6.13.5 การเปลี่ยนแปลงด้านกฎหมาย

6.13.6 การเปลี่ยนแปลงผู้ให้บริการ ผู้รับบริการ และองค์กรภายนอกอื่น ๆ

6.13.7 การเปลี่ยนแปลงกระบวนการใหม่

6.13.8 การเปลี่ยนแปลงความเสี่ยง

7. การกำหนดผู้รับผิดชอบ

กำหนดให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนฉุกเฉินด้าน ICT เป็นผู้มีหน้าที่ดังต่อไปนี้

7.1 ตรวจสอบ บำรุง รักษา แก้ไขข้อบกพร่องต่างๆ ของระบบเครือข่ายและระบบบสารสนเทศของสถาบัน

7.2 จัดให้มีการทำแผนและดำเนินการตามแผนฉุกเฉินด้าน ICT ของสถาบันเพื่อสร้างความต่อเนื่องของการปฏิบัติงาน

ส่วนที่ 12
แนวปฏิบัติในการประเมินความเสี่ยงเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. คำนำ

สถาบันตระหนักถึงความสำคัญของการพัฒนาองค์กรตามแนวทางการบริหารจัดการที่ดี มีธรรมาภิบาล ซึ่งรวมถึงการมีนโยบายและพัฒนาระบบการบริหารความเสี่ยงของสถาบัน เพื่อให้มั่นใจว่าการบริหารความเสี่ยงของสถาบันจะดำเนินการอย่างเป็นระบบ มีความต่อเนื่อง ส่งผลให้การบริหารงานในความรับผิดชอบมีประสิทธิภาพ เกิดประสิทธิผล อำนวยประโยชน์ให้กับชุมชนท้องถิ่นและสังคมตามวัตถุประสงค์และวิสัยทัศน์ขององค์กร ดังที่ได้กำหนดนโยบายบริหารความเสี่ยงไว้แล้ว

สถาบันได้กำหนดกระบวนการบริหารความเสี่ยงและการจัดทำแผนบริหารความเสี่ยงตามกรอบการบริหารความเสี่ยงตามแนวทางของ COSO – ERM (Enterprise Risk Management)

สำหรับกระบวนการบริหารความเสี่ยงทั่วทั้งองค์กรของสถาบัน ซึ่งประกอบด้วยการบริหารความเสี่ยงระดับองค์กรและระดับส่วนงานนั้น มุ่งเน้นให้เกิดผลสำเร็จตามแผนยุทธศาสตร์การดำเนินงาน ดังนั้น โครงการหรือกิจกรรมที่ต้องดำเนินการวิเคราะห์ ประเมิน และบริหารจัดการความเสี่ยง จึงเป็นโครงการหรือกิจกรรมที่ส่วนงานได้จัดทำขึ้นตามแผนปฏิบัติการและแผนงบประมาณ

หลักการสำคัญประการหนึ่งในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศคือการประเมินความเสี่ยงที่อาจเกิดขึ้นและมีผลกระทบทำให้ข้อมูลและระบบข้อมูลมีความไม่มั่นคงปลอดภัยได้ เพื่อให้การประเมินความเสี่ยงสามารถทำได้อย่างมีประสิทธิภาพจำเป็นต้องมีการระบุความเสี่ยงและกำหนดวิธีการประเมินอย่างชัดเจนเป็นระบบ อย่างไรก็ตาม ความเสี่ยงที่อาจเกิดขึ้นได้มีได้หลายประเภท แต่ละประเภทความเสี่ยงก็อาจมีวิธีในการประเมินแตกต่างกันออกไป ดังนั้นอาจจำเป็นต้องระบุและประเมินความเสี่ยงเป็นเรื่อง ๆ ไป

ในการประมวลผลค่าความเสี่ยงอาจจะมีได้หลายวิธีการขึ้นอยู่กับสถานการณ์สภาพแวดล้อมและปัจจัยที่เกี่ยวข้อง ตัวอย่างเช่น การใช้ดุลพินิจพิจารณาจากองค์ประกอบต่าง ๆ เช่น มูลค่าของสินทรัพย์ (Asset Value) ความรุนแรงของผลกระทบที่เกิดขึ้น ภาวะคุกคาม (Threat) และจุดอ่อน (Vulnerability) เป็นต้น หรือโดยวิธีประเมินระดับความเสี่ยงเป็นระดับสูง (H) ระดับปานกลาง (M) และระดับต่ำ (L) นอกจากนี้ยังสามารถประเมินโดยกำหนดเป็นคะแนนให้กับองค์ประกอบที่เกี่ยวข้อง

สำหรับการประเมินผลค่าความเสี่ยงที่ใช้ของสถาบัน ใช้วิธีการประเมินความเสี่ยงโดยคำนึงถึงผลกระทบด้านความสำเร็จ โดยกำหนดเป็นร้อยละของระดับความรุนแรงต่อความสำเร็จของโครงการ

โดยทั่วไปในการให้คะแนนในแต่ละด้าน อาจประเมินโดยใช้วิธีการต่าง ๆ กัน เช่น ประเมินจากดุลพินิจของผู้ที่เกี่ยวข้อง ประเมินโดยผู้เชี่ยวชาญทางด้านนั้น ๆ หรือประเมินโดยการสำรวจข้อมูล เป็นต้น

2. แนวปฏิบัติในการประเมินความเสี่ยงด้านสารสนเทศ

2.1 กำหนดเกณฑ์การประเมินมาตรฐาน โดยพิจารณาเงื่อนไขในการกำหนดเกณฑ์การประเมินความเสี่ยง 2 มิติ คือโอกาสที่จะเกิดความเสี่ยง (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) เพื่อกำหนดระดับความเสี่ยง (Degree of Risks) ของความเสี่ยงแต่ละเหตุการณ์ต่อไป

2.2 ประเมินโอกาสและผลกระทบของความเสี่ยง โดยควรให้ความสำคัญต่อความเสี่ยงที่มีผลกระทบสูงและมีโอกาสเกิดความเสี่ยงสูง เพื่อจัดการความเสี่ยงดังกล่าวก่อน

2.3 จัดลำดับความเสี่ยง เพื่อให้สามารถจัดลำดับความรุนแรงของปัจจัยเสี่ยงที่มีผลกระทบต่อวัตถุประสงค์ของหน่วยงาน และสามารถนำมาพิจารณากำหนดมาตรการควบคุมความเสี่ยงได้อย่างเหมาะสม โดยพิจารณาจากความสัมพันธ์ระหว่างโอกาสที่จะเกิดความเสี่ยงและผลกระทบของความเสี่ยง

2.4 ดำเนินการตามระเบียบ ข้อกำหนด รวมทั้งคำแนะนำตามแผนปฏิบัติการหรือแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศและการสื่อสารที่ได้มีการจัดทำขึ้น เพื่อลดความเสี่ยงและผลกระทบที่มีต่อความเสียหายด้านข้อมูลสารสนเทศอย่างเคร่งครัด

3. การประเมินความเสี่ยง

การประเมินความเสี่ยงเพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศนั้น สถาบันถือเป็นส่วนหนึ่งของการบริหารความเสี่ยงและการจัดทำแผนบริหารความเสี่ยงทั่วทั้งองค์กร ซึ่งมีการปฏิบัติตามกระบวนการอย่างจริงจัง เป็นระบบและมีความต่อเนื่องทุกปีอย่างน้อยปีละ 1 ครั้ง โดยสำนักตรวจสอบ ซึ่งเป็นหน่วยงานภายใน และทุก 3 ปี จะมีการจ้างหน่วยงานภายนอกให้ทำการศึกษาประเมินผลการดำเนินงาน รวมทั้งประมวลผลการดำเนินงานเพื่อจัดทำข้อเสนอเป็นแนวทางในการพัฒนา และปรับปรุงยุทธศาสตร์ของสถาบัน เพื่อใช้เป็นกรอบชี้นำการดำเนินงานต่อไปในอนาคต โดยให้เป็นไปตามแผนปฏิบัติการหรือแผนฉุกเฉินที่ได้กำหนดไว้

การประเมินความเสี่ยงใช้หลักการพิจารณาร่วมกันระหว่างโอกาสความเป็นไปได้ ระดับความเสี่ยง และผลกระทบต่อความเสียหายของสถาบัน พอสรุปดังนี้คือ

โอกาสความเป็นไปได้ (Likely hood) ที่จะเกิดเหตุไม่พึงประสงค์ อาจแบ่งเป็น 4 ระดับ

คะแนน	โอกาสที่จะเกิด Likelihood	ความถี่ที่เกิดขึ้น (เฉลี่ย)
1	น้อย (1)	มีโอกาสเกิดเหตุการณ์น้อยกว่าปีละ 1 ครั้ง
2	ปานกลาง (2)	มีโอกาสเกิดเหตุการณ์ไม่เกิน 2 ครั้งต่อปี
3	ค่อนข้างมาก (3)	มีโอกาสเกิดเหตุการณ์ไม่เกิน 6 ครั้งต่อปี
4	มาก (4)	มีโอกาสเกิดเหตุการณ์มากกว่า 6 ครั้งต่อปี

การประเมินผลกระทบ (Impact)

ระดับความรุนแรง	การเงิน(F)	การปฏิบัติการ(O)	ภาพลักษณ์ (R)	ผู้ใช้บริการ (C)	บุคลากร (E)
1	เสียหายด้านการเงินน้อยกว่า 1 แสนบาท	- ระยะเวลาหยุดชะงักน้อยกว่า 1 ชม.	กระทบชื่อเสียงและภาพพจน์ของสถาบันไม่เป็นข่าวเผยแพร่	ผู้ใช้บริการไม่พอใจแต่ไม่มีเรื่องร้องเรียน	ไม่สูญเสียข้อมูลส่วนบุคคล
2	เสียหายด้านการเงิน 1 แสนบาทแต่ไม่ถึง 5 แสนบาท	-ระยะเวลาหยุดชะงัก 1 ชม.แต่ไม่ถึง 3 ชม.	กระทบชื่อเสียงและภาพพจน์ของสถาบัน ปานกลาง มีการเผยแพร่ข่าวในวงจำกัดภายในประเทศไม่เกิน 1 วัน	ผู้ใช้บริการไม่พอใจมีผู้ร้องเรียนไม่เกิน 5 ราย	
3	เสียหายด้านการเงิน 5 แสนบาทแต่ไม่ถึง 1 ล้านบาท	-ระยะเวลาหยุดชะงัก 3 ชม แต่ไม่ถึง 12 ชม.	กระทบชื่อเสียงและภาพพจน์ของสถาบันค่อนข้างมาก มีการเผยแพร่ข่าวผ่านสื่อภายในประเทศหลายฉบับติดต่อกันไม่เกิน 5 วัน	ผู้ใช้บริการไม่พอใจมีผู้ร้องเรียนมากกว่า 6 รายแต่ไม่เกิน 10 ราย	
4	เสียหายด้านการเงินตั้งแต่ 1 ล้านบาทขึ้นไป	- ระยะเวลาหยุดชะงักตั้งแต่ 12 ชม. ขึ้นไป	กระทบชื่อเสียงและภาพพจน์ของสถาบันค่อนข้างมาก มีการเผยแพร่ข่าวผ่านสื่อทั้งภายในและต่างประเทศ	ผู้ใช้บริการไม่พอใจมีผู้ร้องเรียนตั้งแต่ 10 รายขึ้นไป	ถูกละเมิดสิทธิและสูญเสียข้อมูลส่วนบุคคล

จากโอกาสความเป็นไปได้ที่จะเกิดเหตุไม่พึงประสงค์ ระดับความเสี่ยงที่กำหนดไว้ และผลกระทบ (Effect) ที่อาจเกิดขึ้นได้ สามารถที่จะนำมาจัดทำตารางความสัมพันธ์ (Risk Map) เพื่อความสะดวกต่อการประเมินความเสี่ยง และกำหนดแนวทางบริหารจัดการได้อย่างเหมาะสมต่อไป

ระดับค่าความเสี่ยง (Risk Level)		โอกาสที่จะเกิด (Likelihood Rating)			
		1	2	3	4
ผลกระทบ (Impact Rating)	4	M	H	E	E
	3	M	M	H	E
	2	L	M	M	H
	1	L	L	M	M

ระดับความเสี่ยงได้ถูกกำหนดให้มีจำนวนทั้งนี้ 4 ระดับ ดังนี้

1. ระดับ L หมายความว่า เป็นระดับความเสี่ยงที่น้อย	ยอมรับความเสี่ยง
2. ระดับ M หมายความว่า เป็นระดับความเสี่ยงที่ปานกลาง	ยอมรับความเสี่ยง
3. ระดับ H หมายความว่า เป็นระดับความเสี่ยงที่สูง	จัดทำแผนจัดการความเสี่ยง
4. ระดับ E หมายความว่า เป็นระดับความเสี่ยงที่สูงมาก	จัดทำแผนจัดการความเสี่ยง

แนวทางในการดำเนินการกับความเสี่ยงที่พบ

ระดับความเสี่ยงโดยรวม	แนวทางการดำเนินการ
สูงมาก	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งรัดจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที
สูง	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้ โดยต้องมีการจัดการความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
ปานกลาง	ระดับความเสี่ยงที่พอยอมรับได้ แต่ต้องมีการควบคุม เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
ต่ำ	ระดับความเสี่ยงที่อาจยอมรับได้ แต่อาจจำเป็นต้องมีการควบคุม

การยอมรับความเสี่ยงและการบริหารจัดการของสถาบัน

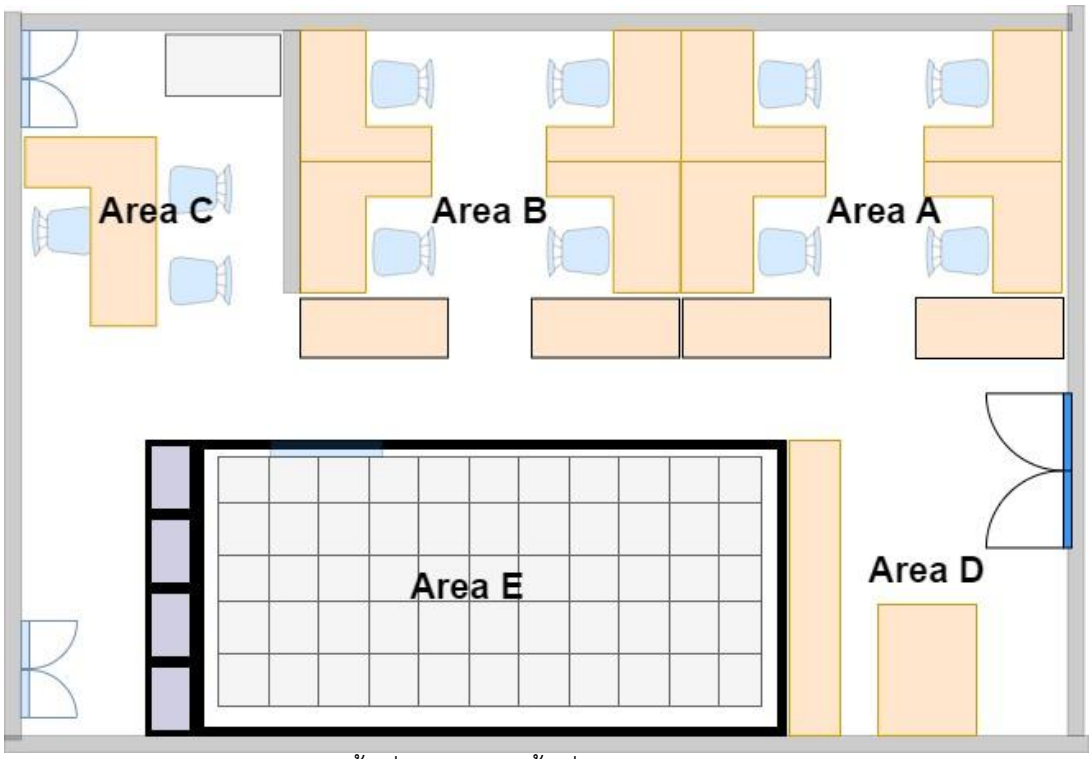
ในทางปฏิบัติการประเมินความเสี่ยงด้านสารสนเทศ และผลกระทบที่เกิดขึ้นต่อสถาบัน ย่อมไม่มีฝ่ายใดที่สามารถจะคาดการณ์ได้อย่างครบถ้วนทุกกรณี และถึงแม้จะมีการคาดการณ์ล่วงหน้าไว้แล้ว แต่หลายกรณีก็ยังมีความจำเป็นต้องยอมรับความเสี่ยงนั้น ด้วยเหตุผลความไม่คุ้มค่าในการลงทุนงบประมาณ เพื่อที่จะป้องกันมิให้เกิดเหตุการณ์เหล่านั้นได้ ดังนั้น การยอมรับความเสี่ยงที่ควบคุมไม่ได้ ไม่มีผู้ใดคาดการณ์ล่วงหน้าได้ หรืออาจไม่คุ้มค่าต่อการลงทุน จึงเป็นสิ่งจำเป็นที่ทุกฝ่ายจะต้องให้ความยินยอม และพร้อมรับผลกระทบที่อาจเกิดขึ้นร่วมกัน โดยอาจจัดให้เป็นกิจกรรมสำคัญในแผนฉุกเฉินด้านสารสนเทศ แต่ก็มิได้หมายความว่าความเสี่ยงทุกอย่างหรือทุกเหตุการณ์ที่เกิดขึ้น จะต้องนำไปเป็นข้อกำหนดหรือประกาศใช้ในแผนฉุกเฉินเสมอไป หากแต่ทุกฝ่ายควรร่วมมือกันเพื่อที่จะลดความเสี่ยง โดยไม่ต้องรอให้เกิดเหตุไม่พึงประสงค์ และสมควรที่จะบริหารจัดการความเสี่ยงอย่างเหมาะสม ซึ่งในที่นี้จะเรียงตามระดับของโอกาสความเป็นไปได้ (Likely hood) และผลกระทบที่มีต่อการดำเนินงานด้านสารสนเทศ เพื่อแสดงให้เห็นภาพรวมแนวทางวิธีการดำเนินงานทั่วไป และมาตรฐานขั้นตอนการปฏิบัติในภาวะฉุกเฉิน โดยเฉพาะอย่างยิ่งประเด็นความเสี่ยงในระดับของ Extreme และ High

ส่วนที่ 13
แนวปฏิบัติการกำหนดพื้นที่เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

1. วัตถุประสงค์

เพื่อเป็นแนวปฏิบัติในการกำหนดพื้นที่เพื่อรักษาความปลอดภัยทางกายภาพสำหรับโครงสร้างและทรัพยากรทางด้านสารสนเทศ รวมถึงการจัดการการเข้าถึงทรัพยากรทางกายภาพโดยมีการอนุญาตให้เฉพาะผู้ที่เกี่ยวข้องและมีความจำเป็นเท่านั้น โดยในที่นี่จะกล่าวถึงเฉพาะในส่วนของห้องสำนักเทคโนโลยีสารสนเทศ

2. แนวปฏิบัติการกำหนดและจัดสรรพื้นที่



แผนภาพแสดงการกำหนดพื้นที่และจัดสรรพื้นที่การใช้งานห้องสำนักเทคโนโลยีสารสนเทศ

จากแผนภาพด้านบน หัวหน้าสำนักเทคโนโลยีสารสนเทศ ต้องกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) และพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

พื้นที่	ชื่อพื้นที่	ลักษณะของพื้นที่			
		พื้นที่ทำงานทั่วไป	พื้นที่ทำงานของผู้ดูแลระบบ	พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ	พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์
Area : A	ส่วนของงานระบบฐานข้อมูล งานบริหารสำนักและหัวหน้างาน	/			
Area : B	ส่วนของงานระบบเทคโนโลยีสารสนเทศ	/	/		
Area : C	ส่วนของผู้บริหาร	/			
Area : D	พื้นที่ที่สำหรับประชุม	/			
Area : E	ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Server Room)		/	/	/

ตารางที่ 1 การกำหนดพื้นที่การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

จากตารางด้านบน แต่ละพื้นที่จะมีการแบ่งลักษณะของพื้นที่ออกเป็น 4 ลักษณะดังนี้ คือ

1. พื้นที่ทำงานทั่วไป คือ พื้นที่ปฏิบัติงานของผู้ปฏิบัติงานสถาบัน แต่ละส่วนงาน ซึ่งเป็นพื้นที่ราชการห้ามบุคคลภายนอกเข้า ยกเว้นกรณีเข้ามาติดต่อราชการ โดยต้องแสดงตนเข้าทำการแลกบัตรผู้ติดต่อและระบุเหตุผลที่เข้ามาติดต่อ

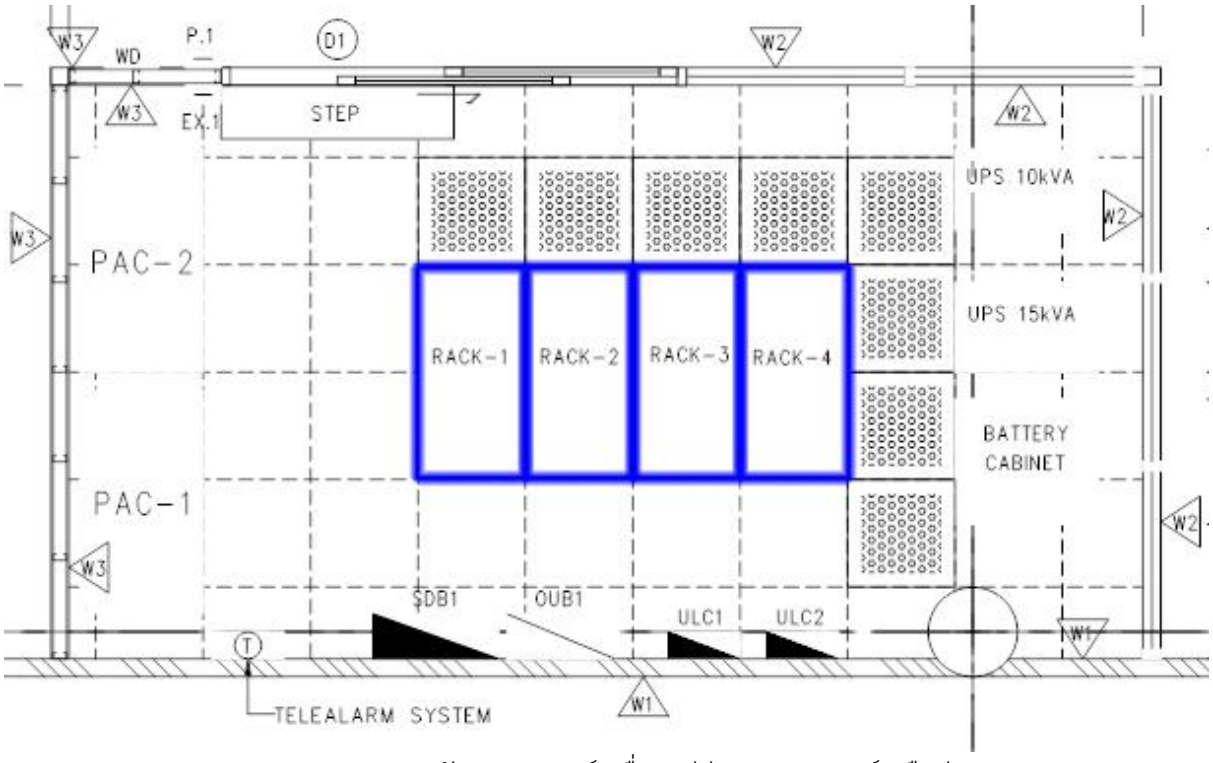
2. พื้นที่ทำงานของผู้ดูแลระบบ คือ พื้นที่ทำงานสำหรับผู้ปฏิบัติงานของสำนักเทคโนโลยีสารสนเทศ ซึ่งได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่ดูแลระบบสารสนเทศ โดยไม่อนุญาตให้ผู้ปฏิบัติงานของสถาบัน ซึ่งสังกัดส่วนงานอื่น ๆ รวมถึงบุคคลภายนอกเข้าพื้นที่ ยกเว้นได้รับการอนุญาตจากเจ้าหน้าที่ผู้ดูแล หรือผู้บังคับบัญชาของสำนักเทคโนโลยีสารสนเทศเท่านั้น

3. พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ คือ พื้นที่หวงห้าม เช่น ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Server Room) ซึ่งอนุญาตให้เฉพาะสำหรับผู้ปฏิบัติงานของสำนักเทคโนโลยีสารสนเทศที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ดูแลเท่านั้น

4. พื้นที่สำหรับประชุมสำนัก คือพื้นที่สำหรับการวางแผนการปฏิบัติงานของสำนักเทคโนโลยีสารสนเทศ

5. พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ คือ พื้นที่ติดตั้งอุปกรณ์จัดเก็บข้อมูลของระบบงานสารสนเทศ ซึ่งมีผู้ปฏิบัติงานของสำนักเทคโนโลยีสารสนเทศผู้ที่ได้รับมอบหมายให้ดูแลระบบสารสนเทศ และได้รับอนุญาตเป็นจากหน่วยงานเจ้าของระบบ ให้เป็นผู้ทำหน้าที่จัดเก็บ สำรองข้อมูลระบบสารสนเทศที่รับผิดชอบดูแล

3. การจัดสรรพื้นที่ภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์



แผนภาพแสดงการจัดวางอุปกรณ์เครื่องแม่ข่ายและอุปกรณ์เครือข่าย
ซึ่งจัดเป็นสัดส่วนในตู้จัดเก็บอุปกรณ์ระบบสารสนเทศ (RACK)
ภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์

จากแผนภาพข้างบน เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ ผู้ที่ได้รับมอบหมายให้ดูแลห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Server Room) ต้องจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น เพื่อความสะดวกและปลอดภัยในการปฏิบัติงาน และยังทำให้การเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

4. การจัดสรรพื้นที่ใช้งานระบบเครือข่ายไร้สาย

สถาบัน มีการให้บริการอินเทอร์เน็ตไร้สายแก่ผู้ปฏิบัติงานและบุคคลภายนอกที่เข้าร่วมกิจกรรมที่จัดขึ้นภายในสถาบัน ครอบคลุมพื้นที่บริเวณอาคารสำนักงาน โดยผู้ใช้งานเครือข่ายจะต้องเข้าใช้ช่องสัญญาณ (SSID) ตามสิทธิที่ได้รับเท่านั้น เช่น CODI_Staff สำหรับเจ้าหน้าที่ CODI_Contractor สำหรับลูกจ้างโครงการผู้ประสาน และ CODI_Guest สำหรับผู้มาติดต่อโดยจะต้องลงทะเบียนการใช้งานผ่านระบบ

5. แนวปฏิบัติสำหรับระบบซึ่งไวต่อการรบกวน

ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสถาบัน ได้แก่ ระบบที่เกี่ยวข้องกับด้านการเงินและงบประมาณ หรือโปรแกรมระบบที่ใช้ในการปฏิบัติงานด้านงบประมาณ ให้ติดตั้งในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ (Server Room) ซึ่งอนุญาตให้เฉพาะสำหรับผู้ปฏิบัติงานของสำนักเทคโนโลยีสารสนเทศที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ดูแลเท่านั้นที่จะสามารถเข้าถึงได้

ส่วนที่ 14
แนวปฏิบัติการบริหารจัดการรหัสผ่าน

1. วัตถุประสงค์

เพื่อเป็นแนวปฏิบัติในการบริหารจัดการรหัสผ่านของผู้ใช้งาน ทั้งในส่วนของการกำหนด เปลี่ยนแปลง ยกเลิกรหัสผ่าน และการทบทวนสิทธิการเข้าถึงระบบสารสนเทศและการสื่อสาร เพื่อให้เกิดความมั่นคงปลอดภัยในการเข้าใช้งานระบบสารสนเทศและการสื่อสาร ซึ่งเป็นข้อมูลที่เป็นความลับส่วนบุคคลและถือว่าเป็นสิทธิและความรับผิดชอบของผู้ใช้งานระบบสารสนเทศที่ต้องปฏิบัติ

2. แนวปฏิบัติการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

2.1 กรณีการเข้าใช้งานระบบโปรแกรมสารสนเทศ ผู้ใช้งานต้องลงนามในแบบฟอร์ม *“ลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ”* ซึ่งเป็นการยอมรับที่จะเก็บรักษารหัสผ่านให้เป็นความลับเฉพาะตน และเก็บรหัสผ่านของกลุ่มไว้เฉพาะสมาชิกในกลุ่ม

2.2 กรณีรหัสผ่านสำหรับระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ผู้ดูแลระบบควรสร้างรหัสผ่านชั่วคราวให้ก่อน ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านทันทีที่เข้าใช้งานระบบครั้งแรก

2.3 ระบบต้องกำหนดกระบวนการเพื่อตรวจสอบตัวตนของผู้ใช้งานก่อนที่จะสร้างรหัสผ่านใหม่ เปลี่ยนรหัสผ่าน หรือรหัสผ่านชั่วคราว

2.4 การส่งรหัสผ่านชั่วคราวให้กับผู้ใช้งาน ควรใช้วิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลที่สามหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

2.5 รหัสผ่านชั่วคราวควรมีความเป็นหนึ่งเดียว ไม่ซ้ำกับคนอื่นและไม่ควรใช้คำที่เดาได้

2.6 ผู้ใช้งานต้องตอบยืนยันการได้รับรหัสผ่านด้วยตัวเอง

2.7 ผู้ใช้งานไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์โดยอยู่ในรูปแบบที่ไม่ได้ป้องกัน

2.8 รหัสผ่านที่กำหนดไว้โดยผู้ผลิตตั้งแต่แรกควรได้รับการตั้งค่าใหม่ทันทีโดยผู้ดูแลระบบหลังจากติดตั้งระบบซอฟต์แวร์

3. แนวปฏิบัติการใช้งานรหัสผ่าน

3.1 ผู้ใช้งานต้องเก็บรหัสผ่านไว้เป็นความลับ

3.2 ผู้ใช้งานต้องหลีกเลี่ยงการบันทึกรหัสผ่าน เช่น บันทึกลงในกระดาษ ในแฟ้มข้อมูล หรือในอุปกรณ์พกพาต่าง ๆ นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัย และวิธีการในการบันทึกได้รับการอนุมัติแล้ว

3.3 ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่า รหัสผ่านอาจรั่วไหล

3.4 กำหนดรหัสผ่านที่มีคุณภาพและมีความยาวที่เหมาะสม ซึ่งต้องคำนึงหลักปฏิบัติ ดังนี้

3.4.1 กำหนดเป็นแบบ complex อย่างน้อย 8 ตัวอักษร โดยต้องมีอักขระพิเศษผสมด้วย

3.4.2 ให้ง่ายสำหรับจดจำ

3.4.3 ไม่ให้อยู่บนพื้นฐานของสิ่งที่ผู้อื่นสามารถคาดเดาได้ง่าย หรือสามารถหาได้จากข้อมูลส่วนตัว เช่น ชื่อ หมายเลขโทรศัพท์ และวันเกิด เป็นต้น

3.4.4 ไม่สร้างจุดอ่อนโดยการใช้คำที่อยู่ในพจนานุกรม

3.4.5 ไม่มีคำซ้ำหรือตัวอักษรซ้ำ ไม่ควรเป็นตัวเลขทั้งหมด หรือไม่ควรเป็นตัวอักษรทั้งหมด

3.5 ผู้ใช้งานควรเปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้งานที่ได้สิทธิพิเศษควรได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ) หรืออย่างน้อยทุก 3 เดือน และหลีกเลี่ยงการวนใช้รหัสผ่านเดิมที่เคยใช้แล้ว

3.6 ระบบควรกำหนดให้เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

3.7 ผู้ใช้งานต้องไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ login อัตโนมัติ

3.8 ผู้ใช้งานต้องไม่ใช้รหัสผ่านร่วมกับผู้อื่น

3.9 ผู้ใช้งานต้องไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ในการปฏิบัติงานและในกรณีใช้ส่วนตัว

3.10 ถ้าผู้ใช้งานจำเป็นต้องเข้าถึงข้อมูล หรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัว ควรแนะนำให้ใช้รหัสผ่านเดียวกันที่มีคุณภาพ โดยปฏิบัติตามข้อ 3.4 ข้างต้นสำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านั้นควรมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

4. แนวปฏิบัติของระบบบริหารจัดการรหัสผ่าน

4.1 ผู้ใช้งานต้องใช้ ID และรหัสผ่านของตนเองในการใช้งานระบบ เพื่อป้องกันการปฏิเสธความรับผิดชอบ

4.2 อนุญาตให้ผู้ใช้งานสามารถกำหนดรหัสผ่านของตนเองได้ และมีกระบวนการตรวจสอบอีกครั้งก่อนยืนยันการเปลี่ยนแปลงรหัสผ่านเพื่อป้องกันความผิดพลาด

4.3 ผู้ใช้งานต้องกำหนดรหัสผ่านที่มีคุณภาพ

4.4 ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านเมื่อเข้าระบบเป็นครั้งแรก

4.5 ผู้ใช้งานควรบันทึกประวัติการเปลี่ยนรหัสผ่านเพื่อป้องกันการใช้ซ้ำ

4.6 ระบบต้องไม่แสดงรหัสผ่านให้เห็นบนหน้าจอ

4.7 ผู้ใช้งานต้องเก็บข้อมูลรหัสผ่านไว้ต่างหากจากข้อมูลอื่น

5. แนวปฏิบัติการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

5.1 ผู้ดูแลระบบจะต้องทำการทบทวนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างสม่ำเสมอ ทุกครั้งที่มีการเปลี่ยนแปลงสิทธิ อันเนื่องมาจากการเปลี่ยนตำแหน่งงานหรือการปรับโครงสร้างการทำงานภายในสถาบัน

5.2 ผู้ดูแลระบบจะต้องทำการเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลเมื่อได้รับการแจ้งจากหน่วยงานที่เกี่ยวข้อง

5.3 ผู้ดูแลระบบจะต้องทำการทบทวนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอสำหรับผู้ได้รับสิทธิพิเศษต้องทบทวนสิทธิการเข้าถึงระบบทุก 3 เดือน

5.4 ผู้ดูแลระบบต้องบันทึกความเปลี่ยนแปลงสิทธิของผู้ใช้งานที่ได้รับสิทธิเข้าใช้งานระบบและผู้ใช้งานที่ได้รับสิทธิพิเศษ

ส่วนที่ 15
แนวปฏิบัติการบริหารจัดการสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์

เพื่อให้มีกระบวนการการกำหนดสิทธิของผู้ใช้งานในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ โดยมีการอนุญาตให้เฉพาะผู้ที่เกี่ยวข้องและมีความจำเป็น

2. การบริหารจัดการสิทธิการใช้งานระบบสารสนเทศ

การใช้งานระบบสารสนเทศและการสื่อสารจำเป็นต้องได้รับสิทธิ กระบวนการที่เกี่ยวข้องกับการบริหารจัดการสิทธิมีดังต่อไปนี้

2.1 การลงทะเบียนขอสิทธิใช้งานระบบเทคโนโลยีสารสนเทศ

2.1.1 กรณีเป็นผู้ปฏิบัติงานของสถาบัน ให้ผู้ใช้งานกรอกข้อมูลลงแบบฟอร์ม *“ขอใช้สิทธิใช้โปรแกรมระบบสารสนเทศของ พอช.”* และให้ผู้อำนวยการสำนัก หรือผู้ช่วยผู้อำนวยการภาค (บริหาร) ให้ความเห็นชอบ แล้วนำส่งสำนักเทคโนโลยีสารสนเทศเพื่อพิจารณาให้สิทธิตามความเหมาะสม

2.1.2 กรณีเป็นบุคคภายนอก ให้ผู้อำนวยการสำนัก หรือผู้ช่วยผู้อำนวยการภาค (บริหาร) ส่งบัญชีรายชื่อผู้ขอใช้สิทธิ พร้อมรายละเอียดส่วนบุคคล มายังสำนักเทคโนโลยีสารสนเทศเพื่อพิจารณาให้สิทธิตามความเหมาะสม

2.2 การให้สิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย จะเป็นผู้พิจารณาอนุญาตการให้สิทธิตามที่ผู้ขอใช้งานเสนอโดย ปฏิบัติตามแนวทางที่ระบุไว้ใน *“แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ” (ส่วนที่ 15)* และ *“แนวปฏิบัติการบริหารจัดการรหัสผ่าน” (ส่วนที่ 14)*

2.3 การแจ้งยกเลิกสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

เมื่อผู้ใช้งานระบบเทคโนโลยีสารสนเทศ ต้องการยกเลิกสิทธิในการเข้าใช้งานระบบที่ได้รับแจ้งบัญชีรายชื่อจากสำนักทรัพยากรบุคคล หรือหัวหน้าหน่วยงานที่เกี่ยวข้อง เห็นว่าผู้ปฏิบัติงานของสถาบันหรือบุคคลภายนอก ที่ได้รับสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศไม่มีความจำเป็นที่จะต้องเข้าใช้งานระบบอีกต่อไป ให้หัวหน้าหน่วยงานนั้น ๆ แจ้งไปยังสำนักเทคโนโลยีสารสนเทศให้ดำเนินการยกเลิกสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

เมื่อสำนักเทคโนโลยีสารสนเทศได้ยกเลิกสิทธิดังกล่าวแล้ว ให้บันทึกประวัติการเปลี่ยนแปลงสิทธิไว้เป็นหลักฐาน

ส่วนที่ 16
แนวปฏิบัติการบริหารจัดการครุภัณฑ์คอมพิวเตอร์และเครือข่าย

1. วัตถุระสงค์

เพื่อช่วยให้เจ้าหน้าที่ผู้ดูแลรับผิดชอบงานในส่วนครุภัณฑ์คอมพิวเตอร์และเครือข่าย สามารถใช้เป็นแนวปฏิบัติในการจัดสรรครุภัณฑ์ให้สอดคล้องกับการดำเนินงานของสถาบันและความต้องการของผู้ใช้งาน รวมถึงการควบคุมทะเบียนและบำรุงรักษาครุภัณฑ์ที่ใช้งานอยู่ในสถาบันได้อย่างมีประสิทธิภาพ ซึ่งนำไปสู่การใช้งานทรัพยากรสารสนเทศที่มีอยู่ในสถาบันได้อย่างมีประสิทธิภาพ เกิดประโยชน์สูงสุด

2. แนวปฏิบัติการลงทะเบียนครุภัณฑ์คอมพิวเตอร์และเครือข่าย

ให้สำนักบริหารงานกลางจัดทำทะเบียน ครุภัณฑ์ที่เกี่ยวกับคอมพิวเตอร์และเครือข่ายตามระบบของสถาบัน และนำส่งให้สำนักเทคโนโลยีสารสนเทศ เพื่อบริหารจัดการในส่วนที่เกี่ยวข้องต่อไป

3. แนวปฏิบัติการเบิกใช้ครุภัณฑ์คอมพิวเตอร์และเครือข่าย

ผู้ใช้งานต้องการใช้งานครุภัณฑ์คอมพิวเตอร์และเครือข่าย ให้ขออนุมัติการยืมและการส่งคืนครุภัณฑ์จากผู้มีอำนาจอนุมัติตามระบบของสถาบัน

4. แนวปฏิบัติการแจ้งซ่อมบำรุงครุภัณฑ์คอมพิวเตอร์และเครือข่าย

4.1 เมื่อผู้ใช้งานพบการทำงานที่ผิดไปจากปกติของครุภัณฑ์ หรือไม่สามารถใช้งานครุภัณฑ์ในการดำเนินงานได้ ผู้ใช้งานต้องทำการปรึกษากับเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศ ที่ทำหน้าที่ให้คำปรึกษาในการแก้ไขปัญหาจากการใช้งานครุภัณฑ์คอมพิวเตอร์และเครือข่ายในเบื้องต้นก่อน หากไม่สามารถแก้ไขปัญหาที่พบได้ ประกอบกับจากการวินิจฉัยปัญหาจากเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศแล้วให้ดำเนินการแจ้งซ่อมบำรุง โดยกรอกข้อมูลครุภัณฑ์ที่ต้องการแจ้งลงใน *“แบบฟอร์มบันทึกแจ้งซ่อมครุภัณฑ์คอมพิวเตอร์ในโปรแกรม Helpdesk”* และยื่นเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการส่งซ่อม

4.2 เจ้าหน้าที่ผู้รับผิดชอบวิเคราะห์อาการเสียหายของครุภัณฑ์จากข้อมูลใน *“แบบฟอร์มบันทึกแจ้งซ่อมครุภัณฑ์คอมพิวเตอร์ในโปรแกรม Helpdesk”* และจากการทดสอบการทำงานด้วยตนเอง รวมถึงพิจารณาข้อมูลประกอบโดยเฉพาะในส่วนของระยะเวลาประกันของครุภัณฑ์ดังกล่าว ซึ่งหากอยู่ในระยะเวลาประกันเจ้าหน้าที่สามารถส่งครุภัณฑ์เข้ารับการซ่อมบำรุงที่ศูนย์บริการของบริษัทผู้ผลิตครุภัณฑ์ได้ โดยไม่เสียค่าใช้จ่ายในส่วนที่ระบุในประกัน หากครุภัณฑ์ดังกล่าวไม่อยู่ในระยะเวลาประกัน เจ้าหน้าที่ผู้รับผิดชอบต้องพิจารณาจากความเสียหายของครุภัณฑ์ หากเสียหายมากอาจจำเป็นจะต้องจำหน่ายครุภัณฑ์ดังกล่าว หรือหากความเสียหายของครุภัณฑ์สามารถแก้ไขได้ให้ดำเนินการแก้ไข

4.3 ในระหว่างที่เจ้าหน้าที่ผู้รับผิดชอบส่งครุภัณฑ์เข้ารับการซ่อมบำรุงนั้น หากมีครุภัณฑ์อื่นที่สามารถใช้งานทดแทนครุภัณฑ์ดังกล่าวได้ ให้เจ้าหน้าที่ดำเนินการแจ้งแก่ผู้ใช้งาน โดยให้ผู้ใช้งานทำเรื่องเบิกใช้งานครุภัณฑ์ โดยกรอกข้อมูลลงใน *“แบบฟอร์มการขอเบิกใช้ครุภัณฑ์คอมพิวเตอร์และเครือข่าย”* โดยระบุรายการ

ครุภัณฑ์ที่ต้องการเบิกใช้รวมถึงสถานที่จัดเก็บหรือติดตั้ง และยื่นเรื่องให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการพิจารณาอนุมัติ และเจ้าหน้าที่ผู้ดูแลทะเบียนครุภัณฑ์ทำการบันทึกข้อมูลครุภัณฑ์ใหม่ลงใน *"แบบฟอร์มทะเบียนครุภัณฑ์คอมพิวเตอร์และเครือข่าย"* เพื่อจัดเก็บเป็นประวัติครุภัณฑ์ของสถาบัน

4.4 หลังจากที่เจ้าหน้าที่ผู้รับผิดชอบส่งครุภัณฑ์ที่พบความเสียหายเข้ารับการแก้ไขเรียบร้อยแล้ว ต้องดำเนินการทดสอบในส่วนที่พบความเสียหายอีกครั้ง ก่อนจัดส่งครุภัณฑ์คืนผู้ใช้งาน โดยเจ้าหน้าที่ผู้รับผิดชอบกรอกข้อมูลรายละเอียดการซ่อมบำรุง และการทดสอบครุภัณฑ์ลงใน *"แบบฟอร์มบันทึกแจ้งซ่อมครุภัณฑ์คอมพิวเตอร์ในโปรแกรม helpdesk"* ในส่วนของเจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ และส่งคืนครุภัณฑ์พร้อมเอกสารดังกล่าวให้กับผู้ใช้งาน

5. แนวปฏิบัติการจำหน่ายครุภัณฑ์คอมพิวเตอร์และเครือข่าย

ในกรณีที่สำนัก/ภาค พบว่าครุภัณฑ์เสียหายเกินกว่าที่จะแก้ไขได้ รวมถึงไม่อยู่ในระยะเวลาประกันหรือเสื่อมสภาพตามอายุการใช้งาน ประกอบกับเมื่อพิจารณาถึงมูลค่าของครุภัณฑ์กับค่าใช้จ่ายในการซ่อมบำรุงแล้ว จำเป็นต้องดำเนินการจำหน่ายครุภัณฑ์ดังกล่าว ให้สำนักเทคโนโลยีสารสนเทศให้ความเห็นประกอบและให้สำนัก/ภาค ดังกล่าว จัดส่งครุภัณฑ์ดังกล่าว ให้กับสำนักบริหารงานกลางดำเนินการตามระเบียบต่อไป

ส่วนที่ 17
แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. วัตถุประสงค์

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจะถูกนำไปปฏิบัติให้เกิดผลได้เพียงใดนั้นขึ้นอยู่กับหลายปัจจัย และปัจจัยที่สำคัญประการหนึ่งก็คือความเข้าใจและความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของบุคลากรที่เกี่ยวข้อง ดังนั้นการเผยแพร่แนวนโยบายและแนวปฏิบัติ การฝึกอบรม เพื่อสร้างความคุ้นเคยกับแนวปฏิบัติ เพื่อสร้างความตระหนักให้กับบุคลากรที่เกี่ยวข้องเป็นเรื่องที่สำคัญ และจำเป็นต้องมีแนวปฏิบัติเพื่อการนั้น

2. แนวทางวิธีการและรูปแบบการสร้างความตระหนัก

สำนักเทคโนโลยีสารสนเทศในฐานะผู้ดูแลความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ควรดำเนินการสร้างความตระหนักรู้แก่บุคลากรอย่างเป็นระบบและหลากหลายรูปแบบ ได้แก่

- **การจัดฝึกอบรมและสัมมนา** เป็นประจำ เพื่อให้ความรู้เกี่ยวกับนโยบายความมั่นคงปลอดภัย แนวทางปฏิบัติที่ถูกต้อง และการรับมือภัยคุกคามทางไซเบอร์ โดยเนื้อหาควรครอบคลุมตั้งแต่พื้นฐานจนถึงกรณีศึกษาและสถานการณ์จริง
- **การประชาสัมพันธ์ผ่านสื่อต่าง ๆ** เช่น จดหมายข่าว อีเมล ภายในองค์กร อินทราเน็ต หรือโปสเตอร์ เพื่อเตือนและกระตุ้นให้บุคลากรตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ
- **การมีข้อสั่งการจากผู้บริหารระดับสูง** เพื่อสร้างความเข้มแข็งในการปฏิบัติตามนโยบายและส่งเสริมวัฒนธรรมความปลอดภัยสารสนเทศในองค์กร
- **การทดสอบและประเมินผลการรับรู้** เช่น การทำแบบทดสอบหรือจำลองสถานการณ์ เพื่อวัดระดับความเข้าใจและความตระหนักของบุคลากร และนำผลไปปรับปรุงการฝึกอบรม
- **การสื่อสารถึงความรับผิดชอบและบทลงโทษ** ในกรณีที่ละเลยหรือฝ่าฝืนนโยบาย เพื่อสร้างแรงจูงใจในการปฏิบัติตามอย่างเคร่งครัด
- **การส่งเสริมให้บุคลากรสังเกตและรายงานเหตุการณ์ผิดปกติ** ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศทันที เพื่อให้หน่วยงานสามารถรับมือและแก้ไขได้อย่างรวดเร็ว

แนวทางเหล่านี้จะช่วยสร้างวัฒนธรรมความปลอดภัยสารสนเทศที่แข็งแกร่งภายในหน่วยงาน และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

3 ข้อเสนอแนะเพิ่มเติม

- ควรมีการจัดทำคู่มือหรือเอกสารสั้น ๆ ที่เข้าใจง่ายสำหรับบุคลากรทุกระดับ
- ใช้เทคโนโลยีช่วย เช่น ระบบ e-Learning หรือแอปพลิเคชันแจ้งเตือน เพื่อให้การเรียนรู้เป็นไปอย่างต่อเนื่องและเข้าถึงง่าย

- ส่งเสริมการแลกเปลี่ยนประสบการณ์และกรณีศึกษาภายในองค์กร เพื่อเพิ่มความรู้และความตระหนักในสถานการณ์จริง
- ติดตามและประเมินผลอย่างสม่ำเสมอ เพื่อปรับปรุงแนวทางการสร้างความตระหนักให้เหมาะสมกับบริบทและเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

ส่วนที่ 18
แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย

1. วัตถุประสงค์

เพื่อควบคุมการเข้าถึงระบบเครือข่ายของสถาบันได้อย่างมีประสิทธิภาพ จำเป็นต้องมีการกำหนดแนวปฏิบัติที่เกี่ยวข้องกับการควบคุมการเข้าถึงระบบเครือข่าย เอกสารฉบับนี้จัดทำขึ้นเป็นแนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายของหน่วยงาน โดยมีการอธิบายแนวปฏิบัติแยกเป็นข้อ ๆ เพื่อสะดวกแก่การนำไปใช้

2. แนวปฏิบัติในการแบ่งแยกเครือข่าย (Segregation in networks)

2.1 ให้มีการแบ่งแยกเครือข่ายออกเป็นส่วน ๆ เพื่อควบคุมการเข้าถึงเครือข่าย ดังนี้

2.1.1 ส่วนที่เป็นสาธารณะ (External Zone)

2.1.2 ส่วนที่เชื่อมต่อภายใน (Internal Zone)

2.1.3 ส่วนที่เชื่อมต่อภายในและที่เป็นสาธารณะ (DMZ Zone)

2.1.4 ส่วนที่เชื่อมต่อเป็นเครือข่ายไร้สาย (Wi-Fi Zone)

2.1.5 ส่วนที่เชื่อมต่อเข้ากับเครือข่ายคลาวด์ (Cloud)

2.2 เพื่อการแบ่งเขตโซนอย่างชัดเจนให้ติดตั้งอุปกรณ์ Gateway กั้นไว้ระหว่างเครือข่ายเพื่อเป็นตัวควบคุมการไหลของข้อมูลระหว่างกัน เช่น Firewall ซึ่งมีการปรับแต่งให้สามารถควบคุมหรือกรองข้อมูลที่สื่อสารกันระหว่างเครือข่ายได้

2.3 การแบ่งแยกส่วนเครือข่ายจะต้องได้รับการพิจารณา รวมถึงเครือข่ายไร้สายจากภายในและจากเครือข่ายส่วนตัว เนื่องจากขอบเขตการเชื่อมต่อของเครือข่ายไร้สายไม่สามารถนิยามให้ชัดเจนได้ ดังนั้นจึงต้องมีการประเมินความเสี่ยงเพื่อหาแนวทางการควบคุมและป้องกัน เช่น การใช้การตรวจสอบตัวตนที่เข้มข้นขึ้น วิธีการเข้ารหัสและการเลือกกำหนดความถี่ช่องสัญญาณเอง เป็นต้น เพื่อที่จะรักษาการแบ่งแยกส่วนได้อย่างปลอดภัยและมีประสิทธิภาพ

3. แนวปฏิบัติการควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control)

3.1 การควบคุมการเชื่อมต่อทางเครือข่าย ผู้ดูแลระบบจะต้องดูแลให้มีการปฏิบัติตาม แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศร และแนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอกสถาบัน ที่ระบุใน *“แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ”* (ส่วนที่ 3)

3.2 ความสามารถในการเชื่อมต่อของผู้ใช้งาน จะต้องถูกจำกัดโดยอุปกรณ์ Gateway ซึ่งจะกรองการรับ-ส่งข้อมูลได้

3.3 ให้มีการจำกัดช่วงเวลาหรือช่วงวันที่ในการอนุญาตให้เชื่อมต่อในกรณีที่มีความจำเป็น

4. แนวปฏิบัติการควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control)

4.1 การควบคุมการกำหนดเส้นทางบนเครือข่าย ผู้ดูแลระบบจะต้องดูแลให้มีการปฏิบัติตามแนวปฏิบัติการบริหารจัดการการเข้าถึงระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ที่ระบุใน *“แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ” (ส่วนที่ 3)*

4.2 การควบคุมเส้นทางสื่อสาร จะต้องอยู่บนพื้นฐานของต้นทางที่สามารถแน่ใจได้และปลายทางที่สามารถตรวจสอบได้

4.3 ใช้อุปกรณ์ Gateway ในการตรวจสอบต้นและปลายทาง ณ จุดควบคุมที่อยู่ระหว่างเครือข่ายภายในและเครือข่ายภายนอก เช่น การใช้ Firewall หรือ proxy เป็นต้น

5. ขั้นตอนปฏิบัติในการเข้าถึงระบบอย่างมั่นคงปลอดภัย (Secure log-on procedures)

5.1 ไม่แสดงเลขที่ระบบหรือเลขที่โปรแกรมจนกว่ากระบวนการ login จะเสร็จสิ้นสมบูรณ์

5.2 แสดงข้อความเตือนว่าคอมพิวเตอร์จะถูกใช้งานโดยผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

5.3 ไม่แสดง help ระหว่างกระบวนการ login ซึ่งอาจเป็นการช่วยให้ผู้ที่ไม่ได้รับอนุญาตค้นหาช่องทางเข้าได้

5.4 ตรวจสอบความถูกต้องของข้อมูลที่ Input เฉพาะเมื่อการ Input เสร็จสิ้นสมบูรณ์แล้ว ถ้ามีความผิดพลาด ระบบต้องไม่แสดงว่าข้อมูลที่ Input ส่วนไหนไม่ถูกต้อง

5.5 จำกัดจำนวนครั้งของการพยายามเข้าใช้ระบบ เช่น ยอมให้ใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง เป็นต้น และจะต้องพิจารณาเพิ่มเติมประเด็นต่อไปนี้

5.5.1 บันทึกการพยายามทั้งที่สำเร็จและไม่สำเร็จ

5.5.2 หลังจากใส่ข้อมูล login ผิดพลาด บังคับระยะเวลาทิ้งช่วงก่อนที่จะยอมให้พยายามครั้งต่อไป

5.5.3 ตัดการเชื่อมโยงเครือข่าย

5.5.4 ส่งข้อความเตือนไปยังหน้าจอของระบบ ถ้ามีความพยายามในการ login หลายครั้งเกินจำนวนครั้งมากที่สุดที่ยอมรับได้

5.5.5 กำหนดรหัสผ่านให้เหมาะสมกับความยาวของรหัสผ่านและมูลค่าของระบบที่จะต้องได้รับการป้องกัน

5.6 จำกัดจำนวนครั้งสูงสุดและจำนวนครั้งต่ำสุดสำหรับกระบวนการ login ถ้าเกินกว่านั้นระบบจะหยุดการให้ login

5.7 แสดงข้อมูลต่อไปนี้หลังจากที่ login สำเร็จแล้ว

5.7.1 วันที่และเวลาของการเข้า login ครั้งที่แล้ว

5.7.2 รายละเอียดของการพยายาม login ที่ไม่สำเร็จตั้งแต่การ login ครั้งที่แล้ว

5.8 ไม่แสดงรหัสผ่านที่ได้ input หรือซ่อนไม่ให้มองเห็นหรือเข้าใจได้

5.9 ไม่ส่งรหัสผ่านผ่านเครือข่ายโดยไม่เข้ารหัสเพื่อรักษาความลับก่อน

6. แนวปฏิบัติในการระบุและพิสูจน์ตัวตนของผู้ใช้งาน (User identification and authentication)

6.1 แนวปฏิบัติดังกล่าวให้ใช้สำหรับผู้ใช้งานทุกประเภท (รวมถึง เจ้าหน้าที่สนับสนุน เจ้าหน้าที่ปฏิบัติการ ผู้บริหารระบบ โปรแกรมเมอร์ระบบ และผู้บริหารฐานข้อมูล)

6.2 ID ของผู้ใช้งานจะถูกใช้เพื่อการติดตามสืบหาร่องรอยกิจกรรมของผู้ใช้งานแต่ละคนได้ภายหลัง

6.3 กิจกรรมงานประจำไม่ควรดำเนินการโดยผู้ใช้งานที่ได้สิทธิพิเศษ

6.4 หากจำเป็นต้องมีการใช้งาน ID ร่วมสำหรับกลุ่มของผู้ใช้งานหรือในเฉพาะบางงาน ในกรณีดังกล่าวต้องมีการจัดทำเอกสารอนุมัติรับรองจากผู้บริหาร ซึ่งจะต้องกำหนดตัวควบคุมอื่นเพิ่มเติมเพื่อดูแลการรับผิดชอบต่อข้อมูลในกรณีใช้ ID ร่วมกัน

6.5 การใช้รหัสผู้ใช้งาน ID ร่วมดังกล่าว จะถูกใช้เฉพาะกรณีที่การใช้งานนั้นไม่จำเป็นต้องบันทึกประวัติการใช้งาน (เช่น การดูอย่างเดียว เป็นต้น) หรือในกรณีที่มีการควบคุมอื่นควบคู่ไปด้วย เช่น อนุญาตให้เข้าใช้เพียงครั้งเดียว

กรณีมีความจำเป็นต้องตรวจยืนยันตัวตนอย่างเข้มข้น อาจใช้วิธีอื่นแทนการใช้รหัสผ่านในการตรวจยืนยันตัวตนได้ เช่น วิธีการใช้การเข้ารหัสเพื่อรักษาความลับ, การยืนยันตัวตนสองชั้น (2FA), Smart Card, Token หรือวิธีการทาง Bio-Metrix

7. แนวปฏิบัติในการพัฒนาระบบบริหารจัดการรหัสผ่าน (Password management system)

กำหนดให้ผู้ใช้งานใช้ ID และรหัสผ่านของตนเองในการใช้งาน สำหรับการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบเครือข่าย ระบบปฏิบัติการ และโปรแกรมประยุกต์และสารสนเทศเพื่อป้องกันการปฏิเสธความรับผิดชอบ (ดูรายละเอียดส่วนที่ 14 แนวปฏิบัติการบริหารจัดการรหัสผ่าน)

8. แนวปฏิบัติในการกำหนดการหมดเวลาการใช้งานระบบสารสนเทศ (Session time-out)

8.1 กำหนดให้แต่ละระบบมีกลไกในการ Clear Session เมื่อไม่ได้มีการใช้งานตามระยะเวลาที่กำหนด (time-out)

8.2 time-out ต้องกำหนดให้เหมาะสมกับ ประเภทข้อมูลที่เกี่ยวข้อง และระบบสารสนเทศนั้น ซึ่งอาจกำหนดไม่เกิน 30 นาที

8.3 บางระบบอาจใช้รูปแบบเพียง clear และ lock หน้าจอโดยไม่ต้องยกเลิก session ก็ได้

9. แนวปฏิบัติการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

ให้มีการจำกัดระยะเวลาการใช้งานเครือข่ายที่เชื่อมต่อที่เพียงพอและเหมาะสมต่อการใช้งานระบบสารสนเทศแต่ละระบบ โดยกำหนดระยะเวลาสำหรับการใช้งานไม่น้อยกว่า 3 ชั่วโมง และตัดการเชื่อมต่อเมื่อไม่มีการใช้งานในช่วงระยะเวลา 10 นาที ทั้งนี้ให้พิจารณาจากระบบสารสนเทศที่มีความเสี่ยงสูง ได้แก่ ระบบที่เกี่ยวข้องกับด้านการเงิน ให้มีการจำกัดระยะเวลาการใช้งานเครือข่ายที่เชื่อมต่อที่สั้นขึ้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

10. แนวปฏิบัติในการแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation)

10.1 จัดลำดับความสำคัญ (sensitivity) ของระบบ application ต้องมีการระบุอย่างชัดเจน และจัดทำเป็นเอกสารโดยเจ้าของระบบ

10.2 เมื่อจำเป็นต้องใช้ระบบร่วมกันกับระบบอื่นหรือผู้ใช้งานอื่น จะต้องมีการระบุความเสี่ยง และมีการยอมรับโดยเจ้าของระบบนั้น

11. แนวปฏิบัติในการป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communications)

11.1 การป้องกันอุปกรณ์สื่อสารประเภทพกพา ให้ปฏิบัติตาม *"แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์แบบพกพา" (ส่วนที่ 6)*

11.2 ผู้ใช้งานต้องดำเนินการเพื่อระมัดระวังเป็นพิเศษตามสมควรในการประมวลผลและการสื่อสารโดยใช้อุปกรณ์มือถือ

11.3 ผู้ใช้งานต้องระมัดระวังในการใช้อุปกรณ์ประมวลผลบนอุปกรณ์มือถือนอกสถานที่ทำงานที่ได้รับการป้องกัน

11.4 ผู้ใช้งานต้องมีระบบป้องกันการเข้าถึงข้อมูลหรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

11.5 ผู้ใช้งานอุปกรณ์มือถือต้องระมัดระวังการแอบดูข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาต

11.6 ผู้ใช้งานต้องมีกระบวนการเพื่ออัพเดตระบบป้องกันซอฟต์แวร์ไม่พึงประสงค์

12. แนวปฏิบัติในการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

12.1 สถาบันอนุญาตกิจกรรมการใช้งานระบบทางไกลให้เฉพาะกิจกรรมที่มีการบริหารจัดการความปลอดภัยที่ดีสอดคล้องกับ *"แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันพัฒนาองค์กรชุมชน"* ซึ่งจัดให้มีการป้องกันที่เหมาะสมต่อการขโมย การเปิดเผยข้อมูล และการเข้าถึงข้อมูลที่ไม่เหมาะสม

12.2 การทำงานทางไกลจะต้องได้รับอนุญาต จากหัวหน้าส่วนงานและมีการควบคุมด้านความปลอดภัยอย่างเหมาะสมจากสำนักเทคโนโลยีสารสนเทศ โดยเฉพาะการเข้าถึงข้อมูลจากระยะไกล (Remote Access)

13. แนวปฏิบัติการใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities)

13.1 เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ ผู้ดูแลระบบจะต้องทำการกำหนดระดับสิทธิของผู้ขอใช้งานโปรแกรมอรรถประโยชน์ เพื่อจำกัดและควบคุมการใช้งาน

13.2 โปรแกรมอรรถประโยชน์ที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของสถาบัน ต้องเป็นโปรแกรมที่สถาบันได้ซื้อลิขสิทธิ์ หรือได้รับอนุญาตอย่างถูกต้องตามกฎหมายเท่านั้น

13.3 มีการจำกัดผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์

13.4 ต้องยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์และซอฟต์แวร์ที่เกี่ยวข้องที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้

ส่วนที่ 19
แนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ แนวทางปฏิบัติที่เกี่ยวข้องกับข้อมูลส่วนบุคคล และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และเพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ และเพื่อให้มีมาตรการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

2. แนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล

ให้เป็นไปตามระเบียบของสถาบันที่ออกตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 โดยมีสาระสำคัญและแนวทางปฏิบัติ ดังนี้

- **การเก็บรวบรวมข้อมูลส่วนบุคคล**
    - ต้องเก็บรวบรวมข้อมูลเท่าที่จำเป็นและสอดคล้องกับวัตถุประสงค์ที่แจ้งเจ้าของข้อมูลไว้ล่วงหน้า
    - ต้องแจ้งเจ้าของข้อมูลให้ทราบถึงวัตถุประสงค์ วิธีการเก็บข้อมูล และสิทธิของเจ้าของข้อมูลก่อนหรือในขณะที่เก็บข้อมูล
    - ห้ามใช้ข้อมูลในวัตถุประสงค์อื่นที่ไม่ได้แจ้งไว้ เว้นแต่ได้รับความยินยอมใหม่จากเจ้าของข้อมูลหรือมีกฎหมายรองรับ
- **การใช้และเปิดเผยข้อมูลส่วนบุคคล**
    - ต้องใช้ข้อมูลตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น
    - ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนเปิดเผยข้อมูลให้บุคคลภายนอก เว้นแต่กฎหมายกำหนดให้เปิดเผยได้
    - ต้องมีมาตรการรักษาความมั่นคงปลอดภัยข้อมูลไม่ให้ถูกเข้าถึง แก้ไข หรือเปิดเผยโดยไม่ได้รับอนุญาต
- **สิทธิของเจ้าของข้อมูลส่วนบุคคล**

  เจ้าของข้อมูลมีสิทธิ์ตามกฎหมาย เช่น
    - สิทธิได้รับแจ้งรายละเอียดการเก็บรวบรวมและใช้ข้อมูล
    - สิทธิขอเข้าถึงและรับสำเนาข้อมูลส่วนบุคคล
    - สิทธิขอแก้ไขข้อมูลที่ไม่ถูกต้อง
    - สิทธิขอให้ลบหรือทำลายข้อมูล
    - สิทธิขอระงับการใช้ข้อมูล
    - สิทธิถอนความยินยอมในการใช้ข้อมูล
    - สิทธิร้องเรียนเมื่อมีการละเมิดข้อมูลส่วนบุคคล

- **หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)**
    - จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลอย่างเหมาะสม
    - จัดทำและบันทึกข้อมูลเกี่ยวกับการประมวลผลข้อมูลส่วนบุคคล
    - แจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลต่อเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและเจ้าของข้อมูลตามระยะเวลาที่กฎหมายกำหนด
    - ให้คำแนะนำและอบรมบุคลากรเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลอย่างต่อเนื่อง
- **การแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)**
    - เพื่อดูแลและประสานงานด้านการคุ้มครองข้อมูลส่วนบุคคลภายในหน่วยงาน
    - ตรวจสอบและประเมินการปฏิบัติตามกฎหมาย PDPA
    - เป็นจุดติดต่อระหว่างหน่วยงาน เจ้าของข้อมูล และหน่วยงานกำกับดูแล
- **มาตรการเยียวยาและบทลงโทษ**
    - กำหนดมาตรการแก้ไขเมื่อเกิดการละเมิดข้อมูลส่วนบุคคล เช่น การแจ้งเตือนเจ้าของข้อมูล การชดเชยความเสียหาย
    - ปฏิบัติตามบทลงโทษทางแพ่ง อาญา และปกครองตามที่กฎหมายกำหนด

แนวปฏิบัติเหล่านี้ช่วยให้หน่วยงานปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 อย่างครบถ้วนและมีประสิทธิภาพ เพื่อคุ้มครองสิทธิของเจ้าของข้อมูล และสร้างความน่าเชื่อถือในการบริหารจัดการข้อมูลส่วนบุคคลขององค์กร

ส่วนที่ 20
แนวปฏิบัติการควบคุมแอพพลิเคชั่น

1. วัตถุประสงค์

เพื่อควบคุมและป้องกันการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยไม่ได้รับอนุญาต

2. แนวทางการควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction)

แนวทางการควบคุมการเข้าถึงสารสนเทศ (Information Access Restriction) ให้ดำเนินการ ดังนี้

2.1 ผู้ดูแลระบบ (Administrator) ต้องจัดให้มีการลงทะเบียนผู้ใช้งาน (User) การกำหนดสิทธิ์ตามตำแหน่งและหน้าที่ที่ได้รับมอบหมาย และการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Right อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ได้แก่ ย้าย ให้โอน ลาออก หรือสิ้นสุดการจ้าง ซึ่งรวมถึงบุคคลภายนอกหรือผู้รับจ้าง (Outsource) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศด้วย

2.2 ผู้ดูแลระบบ (Administrator) ต้องกำหนดให้ผู้ใช้งาน (User) ที่เข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศผ่านเครือข่ายภายนอกให้รับส่งข้อมูลผ่านเครือข่ายส่วนตัวเสมือน (VPN : Visual Private Network) โดยมีการเข้ารหัสรักษาความปลอดภัยแบบ Secure Sockets Layer (SSL)

2.3 ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญเช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

2.4 ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

- กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
- กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง
- กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน
- ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับ
- ความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่า เข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

2.5 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูล

ตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

- ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
- ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล
- กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
- การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น
- กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล
- กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

2.6 ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง ให้ปฏิบัติดังนี้

- แยกระบบที่ไวต่อการรบกวนออกจากระบบงานอื่น ๆ
- มีการควบคุมสภาพแวดล้อมของตนเอง โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน
- มีการกำหนดสิทธิ์ให้เฉพาะผู้ที่มีสิทธิ์ใช้ระบบเท่านั้น

2.7 การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องปฏิบัติดังต่อไปนี้

- ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์
- ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป
- เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที
- เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย
- หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

2.8 การควบคุมการเข้าถึงของผู้รับจ้าง (Outsource) ผ่านระบบ

2.8.1 ก่อนปฏิบัติงาน

- ผู้รับจ้าง (Outsource) ต้องขออนุญาตผู้อำนวยการสำนักเทคโนโลยีสารสนเทศเพื่อเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ โดยกรอกข้อมูลลงในแบบฟอร์มการขออนุญาตเข้าถึงระบบคอมพิวเตอร์ และระบบสารสนเทศสำหรับผู้รับจ้างพร้อมแนบสำเนาสัญญาจ้างหรือเหตุผลในการปฏิบัติงาน
- ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายพิจารณาเหตุผลการขออนุญาตดังกล่าวและต้องอนุมัติเป็นลายลักษณ์อักษร
- ผู้ดูแลระบบ (Administrator)ดำเนินการสร้างบัญชีผู้ใช้งาน (Username) และกำหนดรหัสผ่านชั่วคราว (Temporary Password) สำหรับเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ
- ผู้ดูแลระบบ (Administrator) แจ้งให้ผู้รับจ้าง (Outsource) ได้รับทราบ

2.8.2 ระหว่างปฏิบัติงาน

- ผู้รับจ้าง (Outsource) ต้องติดบัตรแสดงตนตลอดระยะเวลาที่ปฏิบัติงาน
- เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศที่ได้รับมอบหมายจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศต้องกำกับดูแลการปฏิบัติงานของผู้รับจ้าง (Outsource) ตลอดระยะเวลาการดำเนินการ
- ผู้รับจ้าง (Outsource) ต้องปฏิบัติงานตามหน้าที่ที่ได้ รับมอบหมายเท่านั้น และต้องคำนึงถึงการรักษาความลับข้อมูลของทางราชการเป็นสำคัญ หากเกิดปัญหาระหว่างการปฏิบัติงานให้แจ้งเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศที่กำกับดูแลการปฏิบัติงานทันที

2.8.3 หลังปฏิบัติงาน

- ผู้รับจ้าง (Outsource) แจ้งความประสงค์ต่อผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือตัวแทนฝ่ายบริหาร SMR เพื่อยกเลิกสิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศทันทีเมื่อปฏิบัติงานแล้วเสร็จ
- ผู้ดูแลระบบ (Administrator) จะยกเลิกสิทธิ์การเข้าถึงระบบคอมพิวเตอร์และระบบสารสนทศและลบข้อมูลสารสนเทศของผู้รับจ้าง (Outsource) เป็นการถาวรเมื่อพ้นกำหนด 90 วัน

2.8.4 การรักษาความลับ

ผู้รับจ้าง (Outsource) ต้องลงนามในสัญญาหรือข้อตกลงการไม่เปิดเผยข้อมูลของหน่วยงาน โดยสัญญาหรือข้อตกลงดังกล่าว ต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศ

ส่วนที่ 21
แนวปฏิบัติการกำหนดมาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ

1.วัตถุประสงค์

เพื่อเป็นการกำหนดมาตรฐานขั้นต่ำในการบริหารจัดการข้อมูลและระบบสารสนเทศขององค์กรให้มีคุณภาพและความถูกต้อง สร้างความมั่นคงปลอดภัยให้กับข้อมูลและระบบสารสนเทศขององค์กร ป้องกันการเข้าถึง การแก้ไข หรือการทำลายข้อมูลโดยไม่ได้รับอนุญาต การใช้งานข้อมูลและระบบสารสนเทศเป็นไปอย่างมีประสิทธิภาพ สนับสนุนการดำเนินงานและการตัดสินใจขององค์กร สอดคล้องกับกฎหมาย กฎระเบียบและข้อบังคับที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและความมั่นคงปลอดภัยไซเบอร์ สร้างความตระหนักและความเข้าใจให้กับบุคลากรทุกระดับในองค์กรเกี่ยวกับความสำคัญของการปฏิบัติตามมาตรฐานข้อมูลและระบบสารสนเทศ

2. แนวปฏิบัติการกำหนดมาตรฐานขั้นต่ำ

2.1. ด้านข้อมูล (Data Standards)

2.1.1. การจำแนกประเภทข้อมูล (Data Classification)

- ต้องมีการจำแนกประเภทข้อมูลตามระดับความสำคัญ ความลับ และผลกระทบหากข้อมูลรั่วไหล ถูกแก้ไข หรือไม่สามารถใช้งานได้ (เช่น ข้อมูลสาธารณะ ข้อมูลภายใน ข้อมูลลับ ข้อมูลลับมาก)
- เจ้าของข้อมูลมีหน้าที่รับผิดชอบในการจำแนกประเภทข้อมูลของตนเอง

2.1.2. คุณภาพข้อมูล (Data Quality)

- ข้อมูลต้องมีความถูกต้อง (Accuracy) ครบถ้วน (Completeness) เป็นปัจจุบัน (Timeliness) สอดคล้องกัน (Consistency) และมีความน่าเชื่อถือ (Reliability)
- ต้องมีกระบวนการตรวจสอบและปรับปรุงคุณภาพข้อมูลอย่างสม่ำเสมอ

2.1.3. การจัดเก็บและการสำรองข้อมูล (Data Storage and Backup)

- ข้อมูลสำคัญต้องมีการจัดเก็บในที่ปลอดภัยและมีการควบคุมการเข้าถึงตามประเภทของข้อมูล
- ต้องมีแผนและกระบวนการสำรองข้อมูลอย่างสม่ำเสมอและทดสอบการกู้คืนข้อมูลเพื่อให้มั่นใจว่าสามารถกู้คืนข้อมูลได้ในกรณีเกิดเหตุการณ์ไม่คาดฝัน
- ระยะเวลาการจัดเก็บข้อมูล (Data Retention) ต้องสอดคล้องกับข้อกำหนดทางกฎหมายและนโยบายขององค์กร

2.1.4. การเข้าถึงและการใช้ข้อมูล (Data Access and Usage)

- การเข้าถึงข้อมูลต้องเป็นไปตามหลักการ “จำเป็นต้องรู้” (Need-to-know basis) และ “สิทธิเท่าที่จำเป็น” (Least privilege)
- ต้องมีการกำหนดสิทธิ์การเข้าถึงข้อมูลตามบทบาทและความรับผิดชอบของผู้ใช้งาน
- ต้องมีการบันทึก (Log) การเข้าถึงและใช้งานข้อมูลที่สำคัญเพื่อการตรวจสอบ

2.1.5. การทำลายข้อมูล (Data Disposal)

- ข้อมูลที่หมดความจำเป็นในการใช้งานหรือจัดเก็บตามระยะเวลาที่กำหนด ต้องถูกทำลายอย่างปลอดภัยและถูกวิธีตามประเภทของข้อมูล เพื่อป้องกันการรั่วไหลของข้อมูล

2.1.6. การคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection)

- การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ต้องเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
- ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล (หากกฎหมายกำหนด) และแจ้งวัตถุประสงค์ในการประมวลผลข้อมูลอย่างชัดเจน
- ต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม

2.2. ด้านระบบสารสนเทศ (Information System Standards)

2.2.1. ความมั่นคงปลอดภัยของระบบ (System Security)

- ต้องมีการติดตั้งและปรับปรุงซอฟต์แวร์ป้องกันไวรัสและมัลแวร์อย่างสม่ำเสมอ
- ต้องมีการบริหารจัดการช่องโหว่ (Vulnerability Management) ของระบบและซอฟต์แวร์
- ต้องมีการใช้ Firewall และระบบตรวจจับการบุกรุก (Intrusion Detection/ Prevention System) ที่เหมาะสม
- ต้องมีการกำหนดค่าความปลอดภัยของระบบ (Secure Configuration) ให้เป็นไปตามมาตรฐานที่องค์กรกำหนด

2.2.2. การบริหารจัดการการเข้าถึงระบบ (Access Control Management)

- ต้องมีการกำหนดนโยบายรหัสผ่านที่รัดกุม (Strong Password Policy) เช่น ความยาวขั้นต่ำการผสมอักขระพิเศษ การเปลี่ยนรหัสผ่านตามกำหนด
- ต้องมีการใช้ระบบยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) สำหรับระบบที่สำคัญ
- ต้องมีการทบทวนสิทธิ์การเข้าถึงระบบของผู้ใช้งานอย่างสม่ำเสมอ และยกเลิกสิทธิ์เมื่อไม่มีความจำเป็น

2.2.3. การพัฒนาระบบสารสนเทศ (System Development)

- การพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงระบบเดิม ต้องคำนึงถึงความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการออกแบบ (Security by Design)
- ต้องมีการทดสอบความปลอดภัย (Security Testing) ก่อนนำระบบขึ้นใช้งานจริง
- การจัดซื้อจัดจ้างระบบสารสนเทศต้องพิจารณาคุณสมบัติด้านความมั่นคงปลอดภัยเป็นสำคัญ

2.2.4. การบริหารจัดการการเปลี่ยนแปลง (Change Management)

- การเปลี่ยนแปลงใด ๆ ที่เกิดขึ้นกับระบบสารสนเทศต้องผ่านกระบวนการขออนุมัติ ทดสอบ และประเมินผลกระทบอย่างเหมาะสม
- ต้องมีการบันทึกรายละเอียดการเปลี่ยนแปลงเพื่อการตรวจสอบย้อนหลัง

2.2.5. การบริหารจัดการเหตุการณ์ผิดปกติและภัยคุกคามทางไซเบอร์ (Incident and Cyber Threat Management)

- ต้องมีแผนและกระบวนการตอบสนองต่อเหตุการณ์ผิดปกติและภัยคุกคามทางไซเบอร์ (Incident Response Plan)
- ต้องมีการฝึกอบรมบุคลากรให้สามารถรับมือกับเหตุการณ์ดังกล่าวได้อย่างถูกต้องและทันท่วงที
- ต้องมีการรายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัยต่อผู้บริหารและหน่วยงานที่เกี่ยวข้องตามที่กฎหมายกำหนด

2.2.6. ความต่อเนื่องทางธุรกิจ (Business Continuity) และการกู้คืนระบบ (Disaster Recovery)

- ต้องมีแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และแผนการกู้คืนระบบ (Disaster Recovery Plan: DRP) สำหรับระบบสารสนเทศที่สำคัญ
- ต้องมีการทดสอบแผน BCP และ DRP อย่างสม่ำเสมอ

3. บทบาทและความรับผิดชอบ

ผู้บริหารระดับสูง: ให้การสนับสนุนทรัพยากรและผลักดันให้เกิดการปฏิบัติตามนโยบายนี้ทั่วทั้งองค์กร

ฝ่ายเทคโนโลยีสารสนเทศ (หรือหน่วยงานที่รับผิดชอบ)

- พัฒนากระบวนการและแนวทางปฏิบัติโดยละเอียดเพื่อให้สอดคล้องกับนโยบายนี้
- ให้คำปรึกษาและสนับสนุนทางเทคนิคแก่หน่วยงานต่าง ๆ
- ติดตามและประเมินการปฏิบัติตามนโยบาย
- ดูแลและบำรุงรักษาระบบสารสนเทศให้มีความมั่นคงปลอดภัยตามมาตรฐาน

เจ้าของข้อมูล

- รับผิดชอบในการจำแนกประเภทข้อมูล
- กำหนดสิทธิ์การเข้าถึงข้อมูล
- ดูแลคุณภาพของข้อมูลที่ตนรับผิดชอบ

ผู้ใช้งานระบบ (Users)

- ปฏิบัติตามนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการใช้งานข้อมูลและระบบสารสนเทศ
- รักษารหัสผ่านของตนเองให้เป็นความลับ
- รายงานเหตุการณ์ผิดปกติหรือข้อสงสัยด้านความปลอดภัยต่อผู้รับผิดชอบทันที

ฝ่ายตรวจสอบภายใน (Internal Audit) ตรวจสอบการปฏิบัติตามนโยบายนี้อย่างสม่ำเสมอ

4. การฝึกอบรมและสร้างความตระหนัก

สถาบันจะจัดให้มีการฝึกอบรมและสร้างความตระหนักเกี่ยวกับนโยบายนี้ รวมถึงแนวปฏิบัติที่ดีด้านความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ ให้แก่บุคลากรทุกระดับอย่างสม่ำเสมอ

ส่วนที่ 22

แนวปฏิบัติการใช้งาน Generative AI

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการในการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence : AI) และ Generative AI ของสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) ให้เป็นไปอย่างเหมาะสม มั่นคงปลอดภัย และสอดคล้องกับภารกิจของสถาบัน รวมถึงส่งเสริมให้ผู้ปฏิบัติงานสามารถนำเทคโนโลยี AI มาใช้สนับสนุนการปฏิบัติงาน การวิเคราะห์ข้อมูล การสืบค้นข้อมูล และการจัดทำเอกสารได้อย่างมีประสิทธิภาพ ภายใต้กรอบกฎหมาย จริยธรรม และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง ตลอดจนเพื่อป้องกันและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ การรั่วไหลของข้อมูล การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และความเสี่ยงที่อาจเกิดจากการใช้งาน AI หรือ Cloud Service ภายนอกองค์กร รวมทั้งเพื่อคุ้มครองข้อมูลส่วนบุคคล ข้อมูลสำคัญของสถาบัน และข้อมูลของประชาชนหรือขบวนองค์กรชุมชน ให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รวมถึงกฎหมาย ระเบียบ และมาตรฐานที่เกี่ยวข้อง พร้อมทั้งกำหนดหลักเกณฑ์ในการกำกับดูแล ตรวจสอบ และติดตามการใช้งาน AI ภายในองค์กร ให้สามารถตรวจสอบย้อนหลังได้ และรองรับการประเมินหรือตรวจสอบจากหน่วยงานภายนอก รวมถึงส่งเสริมการใช้งาน AI อย่างมีความรับผิดชอบ โปร่งใส ตรวจสอบได้ และคำนึงถึงผลกระทบต่อองค์กร บุคลากร และประชาชนผู้รับบริการ

2. แนวทางการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (AI)

2.1 หลักการทั่วไป

- การใช้งาน AI เป็นเพียงเครื่องมือสนับสนุนการปฏิบัติงาน โดยผู้ปฏิบัติงานยังคงต้องรับผิดชอบต่อการตรวจสอบ พิจารณา และตัดสินใจในผลลัพธ์ก่อนนำไปใช้งานจริง
- ผู้ปฏิบัติงานสามารถใช้ AI เพื่อสนับสนุนการปฏิบัติงาน เช่น การสรุปข้อมูล การเรียบเรียงเอกสาร การวิเคราะห์ข้อมูล การค้นคว้าข้อมูล และการสนับสนุนภารกิจของสถาบัน โดยต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ และจริยธรรมขององค์กร
- การใช้งาน AI ต้องคำนึงถึงความมั่นคงปลอดภัยของข้อมูล ความถูกต้องของข้อมูล ความโปร่งใส และผลกระทบที่อาจเกิดขึ้นต่อองค์กรและประชาชน

2.2 การควบคุมและคัดกรองข้อมูลก่อนใช้งาน AI

- ห้ามนำข้อมูลลับ ข้อมูลสำคัญของสถาบัน ข้อมูลส่วนบุคคล หรือข้อมูลอ่อนไหวเข้าสู่ระบบ AI หรือ Cloud Service ภายนอกองค์กร เว้นแต่ได้รับอนุญาตตามกระบวนการที่สถาบันกำหนด และมีมาตรการคุ้มครองข้อมูลที่เหมาะสม

- ห้ามนำข้อมูลที่เกี่ยวข้องกับรหัสผ่าน ระบบรักษาความปลอดภัย API Key ข้อมูลทางการเงิน ข้อมูลบุคลากร ข้อมูลด้านสินเชื่อ หรือข้อมูลของขบวนองค์กรชุมชนเข้าสู่ระบบ AI สาธารณะโดยเด็ดขาด
- กรณีมีความจำเป็นต้องใช้ AI วิเคราะห์ข้อมูล ผู้ปฏิบัติงานต้องดำเนินการปกปิด แทนค่า หรือแปลงข้อมูลส่วนบุคคล (Data Anonymization) ก่อนทุกครั้ง
- ผู้ปฏิบัติงานต้องพิจารณาระดับชั้นความลับและประเภทของข้อมูลก่อนนำข้อมูลเข้าสู่ระบบ AI ทุกครั้ง

2.3 การเลือกใช้ระบบ AI

- การใช้งาน AI ต้องเป็นระบบหรือบริการที่ได้รับอนุญาตจากสถาบัน หรือผ่านการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศแล้ว
- ห้ามติดตั้งหรือใช้งานระบบ AI ที่ไม่ทราบแหล่งที่มา ไม่มีมาตรฐานความปลอดภัย หรืออาจก่อให้เกิดความเสี่ยงต่อระบบสารสนเทศของสถาบัน
- การใช้งาน AI ภายนอกองค์กรต้องคำนึงถึงเงื่อนไขการให้บริการ การจัดเก็บข้อมูล และประเทศที่จัดเก็บข้อมูลของผู้ให้บริการ

2.4 การตรวจสอบผลลัพธ์จาก AI

- ผู้ปฏิบัติงานต้องตรวจสอบความถูกต้อง ความครบถ้วน และความเหมาะสมของผลลัพธ์ที่ได้จาก AI ก่อนนำไปใช้งาน เผยแพร่ หรือใช้อ้างอิงในเอกสารราชการ
- ห้ามใช้ผลลัพธ์จาก AI โดยปราศจากการตรวจสอบจากมนุษย์ (Human-in-the-loop)
- ผู้ปฏิบัติงานต้องตรวจสอบความถูกต้องของข้อมูล ข้อเท็จจริง ตัวเลข แหล่งอ้างอิง และพิจารณาความเสี่ยงด้านข้อมูลบิดเบือน (Hallucination) หรืออคติของ AI ก่อนใช้งาน

2.5 การใช้งานที่ต้องห้าม

- ห้ามใช้ AI เพื่อสร้าง เผยแพร่ หรือสนับสนุนข้อมูลอันเป็นเท็จ ข้อมูลบิดเบือน หรือข้อมูลที่ก่อให้เกิดความเสียหายต่อองค์กร บุคคล หรือสังคม
- ห้ามใช้ AI เพื่อประโยชน์ส่วนตัว หรือกิจกรรมที่ขัดต่อผลประโยชน์ของสถาบัน
- ห้ามใช้ AI ในลักษณะที่ละเมิดลิขสิทธิ์ เครื่องหมายการค้า หรือทรัพย์สินทางปัญญาของผู้อื่น
- ห้ามใช้ AI เพื่อเข้าถึง ทดสอบ หรือโจมตีระบบสารสนเทศโดยไม่ได้รับอนุญาต

2.6 การกำกับดูแลและการตรวจสอบ

- สถาบันอาจมีการบันทึก ตรวจสอบ และติดตามการใช้งาน AI เพื่อประโยชน์ด้านความมั่นคงปลอดภัยสารสนเทศ การบริหารจัดการความเสี่ยง และการตรวจสอบภายใน

- ผู้ปฏิบัติงานต้องให้ความร่วมมือในการตรวจสอบการใช้งาน AI และปฏิบัติตามมาตรการหรือข้อกำหนดที่สถาบันกำหนด
- หน่วยงานด้านเทคโนโลยีสารสนเทศสามารถกำหนดมาตรการเพิ่มเติม ระงับ หรือจำกัดการใช้งาน AI บางประเภทได้ หากพบว่ามีความเสี่ยงต่อองค์กร

2.7 การรายงานเหตุการณ์ผิดปกติ

หากพบเหตุการณ์ผิดปกติ การรั่วไหลของข้อมูล หรือความเสี่ยงด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับการใช้งาน AI ผู้ปฏิบัติงานต้องดำเนินการ ดังนี้

- หยุดการใช้งานระบบหรือบริการดังกล่าวทันที
- แจ้งหน่วยงานด้านเทคโนโลยีสารสนเทศของสถาบันโดยเร็วที่สุด
- รวบรวมข้อมูลและรายละเอียดของเหตุการณ์ เพื่อใช้ในการตรวจสอบ วิเคราะห์ และปรับปรุงมาตรการป้องกันความเสี่ยงขององค์กรต่อไป

ส่วนที่ 23
แนวปฏิบัติการใช้งานระบบคลาวด์ (Cloud Service)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางและมาตรการในการใช้บริการระบบคลาวด์ (**Cloud Service**) ของหน่วยงานภายนอกเป็นโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของสถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) ให้มีความมั่นคงปลอดภัย สามารถรองรับการให้บริการระบบสารสนเทศและภารกิจของสถาบันได้อย่างต่อเนื่อง มีประสิทธิภาพ และสอดคล้องกับกฎหมาย ระเบียบ มาตรฐาน และแนวปฏิบัติด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง รวมถึงเพื่อสนับสนุนการบริหารจัดการระบบสารสนเทศ การจัดเก็บข้อมูล การสำรองและกู้คืนข้อมูล การบริหารจัดการความต่อเนื่องทางธุรกิจ และการให้บริการระบบดิจิทัลของสถาบันในสภาพแวดล้อมด้านเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง

ทั้งนี้ เพื่อป้องกันและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ การสูญหายของข้อมูล การรั่วไหลของข้อมูล การหยุดชะงักของระบบ และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต รวมถึงรองรับการตรวจสอบ การกำกับดูแล และการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรให้เป็นไปอย่างเหมาะสม โปร่งใส และสามารถตรวจสอบย้อนหลังได้

2. มาตรการควบคุมด้านความมั่นคงปลอดภัยสำหรับระบบคลาวด์

2.1 การควบคุมการเข้าถึงและการยืนยันตัวตน (**Access Control & MFA**)

- การยืนยันตัวตนแบบหลายปัจจัย (**Multi-Factor Authentication: MFA**) สถาบันกำหนดให้บัญชีผู้ใช้งานที่มีสิทธิพิเศษ (**Privileged Accounts**) บัญชีผู้ดูแลระบบ (**Administrator Accounts**) และบัญชีที่สามารถเข้าถึงระบบบริหารจัดการคลาวด์ (**Cloud Management Console**) ต้องเปิดใช้งานการยืนยันตัวตนแบบหลายปัจจัย (**MFA**) อย่างน้อย 2 ปัจจัย เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต
- การบริหารจัดการสิทธิ์การเข้าถึง การกำหนดสิทธิ์ในการเข้าถึงและบริหารจัดการระบบคลาวด์ต้องยึดหลักสิทธิเท่าที่จำเป็น (**Principle of Least Privilege**) และกำหนดสิทธิ์ตามหน้าที่ความรับผิดชอบ (**Need-to-Know Basis**) โดยต้องมีการทบทวนสิทธิ์ผู้ใช้งานและผู้ดูแลระบบอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงบุคลากร หน้าที่หรือสถานะการปฏิบัติงาน
- การใช้งานบัญชีผู้ดูแลระบบ บัญชีผู้ดูแลระบบต้องแยกจากบัญชีผู้ใช้งานทั่วไป และห้ามใช้บัญชีร่วมกัน (**Shared Account**) เว้นแต่มีเหตุจำเป็นและต้องสามารถตรวจสอบย้อนหลังได้

2.2 การจำแนกข้อมูลและการคุ้มครองข้อมูล (**Data Classification & Protection)**

ก่อนนำข้อมูลหรือระบบงานขึ้นใช้งานบนระบบคลาวด์ ต้องมีการประเมินประเภทข้อมูล ระดับชั้นความลับ ความสำคัญของข้อมูล และความเสี่ยงที่เกี่ยวข้อง เพื่อกำหนดมาตรการควบคุมด้านความมั่นคงปลอดภัยที่เหมาะสม

ข้อมูลสำคัญ ข้อมูลส่วนบุคคล หรือข้อมูลที่มีกฎหมายกำหนดเป็นการเฉพาะ ต้องได้รับการอนุมัติจากหน่วยงานที่รับผิดชอบก่อนนำขึ้นจัดเก็บหรือประมวลผลบนระบบคลาวด์

ข้อมูลที่จัดเก็บหรือรับส่งผ่านระบบคลาวด์ต้องมีมาตรการเข้ารหัสข้อมูลอย่างเหมาะสม ทั้งในระหว่างการรับส่งข้อมูลผ่านเครือข่าย (**Encryption in Transit)** และระหว่างการจัดเก็บข้อมูล (**Encryption at Rest)** ข้อมูลของสถาบันยังคงถือเป็นทรัพย์สินของสถาบัน แม้จะมีการจัดเก็บหรือประมวลผลผ่านระบบ **Cloud Service** ของหน่วยงานภายนอกก็ตาม

2.3 ขอบเขตความรับผิดชอบระหว่างสถาบันและผู้ให้บริการ (**Shared Responsibility Model)**

สถาบันต้องจัดทำเอกสารกำหนดขอบเขตความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศร่วมกับผู้ให้บริการระบบคลาวด์ให้ชัดเจน โดยครอบคลุมทั้งส่วนที่ผู้ให้บริการรับผิดชอบ เช่น โครงสร้างพื้นฐาน ระบบเครือข่าย และศูนย์ข้อมูล รวมถึงส่วนที่สถาบันรับผิดชอบ เช่น ระบบปฏิบัติการ ระบบงาน ข้อมูล การกำหนดสิทธิ์ และการควบคุมการเข้าถึง

การเลือกใช้ผู้ให้บริการ **Cloud Service** ต้องพิจารณาจากมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ความน่าเชื่อถือของผู้ให้บริการ ความสามารถในการสำรองและกู้คืนข้อมูล การบริหารจัดการความต่อเนื่องของบริการ การป้องกันการรั่วไหลของข้อมูล รวมถึงสถานที่จัดเก็บข้อมูล และความสามารถในการตรวจสอบย้อนหลังได้

ผู้ให้บริการระบบคลาวด์ต้องมีมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศที่เหมาะสม เช่น **ISO/IEC** 27001**, ISO/IEC** 27017 หรือมาตรฐานอื่นที่เกี่ยวข้อง และสถาบันต้องมีการทบทวนความเหมาะสมของผู้ให้บริการเป็นระยะ

2.4 การเฝ้าระวัง ตรวจสอบ และจัดเก็บบันทึกเหตุการณ์ (**Monitoring & Logging)**

ระบบคลาวด์ที่ใช้งานต้องสามารถจัดเก็บบันทึกเหตุการณ์การใช้งานระบบ (**Log)** และเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศได้อย่างเหมาะสม โดยต้องสามารถตรวจสอบ วิเคราะห์ และติดตามเหตุการณ์ย้อนหลังได้ตามระยะเวลาที่สถาบันกำหนด

สำนักเทคโนโลยีสารสนเทศต้องมีการเฝ้าระวังและติดตามเหตุการณ์ผิดปกติ หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อระบบคลาวด์และข้อมูลของสถาบัน รวมถึงต้องมีมาตรการแจ้งเตือนและตอบสนองต่อเหตุการณ์อย่างเหมาะสม

2.5 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย (**Incident Management**)

สถาบันต้องมีขั้นตอนการปฏิบัติงานมาตรฐาน (**Standard Operating Procedure: SOP**) สำหรับการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์และเหตุฉุกเฉินที่เกี่ยวข้องกับระบบคลาวด์ เพื่อให้สามารถตอบสนอง แก้ไข และกู้คืนระบบได้อย่างเหมาะสมและทันเวลา

ในกรณีที่เกิดเหตุละเมิดข้อมูลหรือเหตุภัยคุกคามไซเบอร์ที่ส่งผลกระทบต่อระบบคลาวด์ ผู้ให้บริการและสถาบันต้องมีกลไกการแจ้งเหตุและประสานงานระหว่างกันอย่างรวดเร็ว เพื่อให้สามารถดำเนินการตามกฎหมาย และแจ้งหน่วยงานกำกับดูแลที่เกี่ยวข้องภายในระยะเวลาที่กำหนด

2.6 การสำรองข้อมูลและการกู้คืนระบบ (**Backup & Recovery**)

ข้อมูลสำคัญที่จัดเก็บหรือประมวลผลบนระบบคลาวด์ต้องมีการสำรองข้อมูลตามรอบระยะเวลาที่กำหนด และต้องกำหนดค่าเป้าหมายระยะเวลาการกู้คืนระบบ (**Recovery Time Objective: RTO**) และค่าเป้าหมายจุดกู้คืนข้อมูล (**Recovery Point Objective: RPO**) ให้เหมาะสมกับระดับความสำคัญของระบบงาน

สำนักเทคโนโลยีสารสนเทศต้องมีการทดสอบการกู้คืนข้อมูลและระบบ (**Backup and Recovery Testing**) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าสามารถกู้คืนระบบและข้อมูลกลับมาใช้งานได้จริงภายในระยะเวลาที่กำหนด

2.7 การยกเลิกการใช้งานและการทำลายข้อมูล (**Termination & Data Disposal**)

เมื่อสิ้นสุดการใช้งานระบบคลาวด์ หรือมีการเปลี่ยนแปลงผู้ให้บริการ สถาบันต้องสามารถเรียกคืนข้อมูล ลบข้อมูล หรือทำลายข้อมูลจากระบบของผู้ให้บริการได้อย่างเหมาะสม และต้องมั่นใจว่าข้อมูลของสถาบันไม่ตกค้างอยู่ในระบบของผู้ให้บริการโดยไม่ได้รับอนุญาต

3. แนวทางการใช้งานระบบคลาวด์ (Cloud Service)

สถาบันอาจใช้บริการระบบคลาวด์ (**Cloud Service**) ของหน่วยงานภายนอกเป็นโครงสร้างพื้นฐานในการให้บริการระบบสารสนเทศ ระบบฐานข้อมูล ระบบเว็บไซต์ ระบบสำรองข้อมูล ระบบเฝ้าระวังและวิเคราะห์ข้อมูล รวมถึงระบบดิจิทัลอื่นขององค์กร เพื่อเพิ่มประสิทธิภาพ ความยืดหยุ่น และความต่อเนื่องในการให้บริการ โดยการใช้งานดังกล่าวต้องอยู่ภายใต้การกำกับดูแลของสำนักเทคโนโลยีสารสนเทศ และต้องผ่านการประเมินความเหมาะสมด้านความมั่นคงปลอดภัยสารสนเทศ การบริหารจัดการความเสี่ยง และความพร้อมในการให้บริการของผู้ให้บริการก่อนนำมาใช้งาน

ก่อนนำระบบหรือข้อมูลขึ้นใช้งานบน **Cloud Service** ต้องได้รับการพิจารณาและอนุมัติจากหน่วยงานที่รับผิดชอบด้านเทคโนโลยีสารสนเทศของสถาบัน โดยต้องมีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และผลกระทบที่อาจเกิดขึ้นต่อองค์กร เพื่อกำหนดมาตรการควบคุมที่เหมาะสม

ผู้ปฏิบัติงานต้องใช้งานระบบคลาวด์ภายใต้ขอบเขตอำนาจหน้าที่และสิทธิ์ที่ได้รับเท่านั้น และต้องปฏิบัติตามมาตรการด้านความมั่นคงปลอดภัยสารสนเทศของสถาบันอย่างเคร่งครัด

ห้ามผู้ปฏิบัติงานนำข้อมูลของสถาบันไปจัดเก็บ เผยแพร่ หรือประมวลผลผ่าน **Cloud Service** ส่วนบุคคล หรือระบบที่ไม่ได้รับอนุญาตจากสำนักเทคโนโลยีสารสนเทศ

ห้ามดำเนินการใด ๆ ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ การให้บริการขององค์กร หรือก่อให้เกิดความเสียหายต่อข้อมูลของสถาบัน

หากพบเหตุการณ์ผิดปกติ การรั่วไหลของข้อมูล หรือเหตุการณ์ที่อาจส่งผลกระทบต่อระบบคลาวด์และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ผู้ปฏิบัติงานต้องแจ้งสำนักเทคโนโลยีสารสนเทศทันที เพื่อดำเนินการตรวจสอบ บริหารจัดการเหตุการณ์ และลดผลกระทบที่อาจเกิดขึ้นต่อองค์กรต่อไป

ภาคผนวก

สัญญาการไม่เปิดเผยข้อมูลของสถาบัน

ข้อแนะนำในการทำสัญญาให้เก็บรักษาข้อมูลไว้เป็นความลับ

1. จัดทำสัญญาสัญญาให้เก็บรักษาข้อมูลไว้เป็นความลับให้เรียบร้อย **ก่อน**ที่จะมีการเริ่มพูดคุยกัน
2. หากมีผู้ให้ข้อมูลหลายท่าน **ให้ทุกท่านลงนาม** โดยระบุดังนี้
   2.1 *(ชื่อผู้ให้ข้อมูล 1)*..... อยู่ที่..... เบอร์โทร.....
   2.2 *(ชื่อผู้ให้ข้อมูล 2)*..... อยู่ที่..... เบอร์โทร.....
   2.3 *(ชื่อผู้ให้ข้อมูล 3)*..... อยู่ที่..... เบอร์โทร.....
3. หากมีผู้รับข้อมูลหลายท่าน **ให้ทุกท่านลงนาม** โดยระบุดังนี้
   3.1 *(ชื่อผู้รับข้อมูล 1)*..... อยู่ที่..... เบอร์โทร.....
   3.2 *(ชื่อผู้รับข้อมูล 2)*..... อยู่ที่..... เบอร์โทร.....
   3.3 *(ชื่อผู้รับข้อมูล 3)*..... อยู่ที่..... เบอร์โทร.....
4. ในทางกลับกัน หากบริษัทเป็นผู้ให้ข้อมูล หรือให้โจทย์วิจัย และต้องการโจทย์นั้นเป็นความลับทางธุรกิจ ให้เป็นผู้รับข้อมูล และบริษัทเป็นผู้ให้ข้อมูล
5. สัญญานี้ควรจัดทำขึ้น**สองฉบับ**มีข้อความถูกต้องตรงกัน และคู่สัญญาต่างเก็บไว้ฝ่ายละฉบับ

** หากมีประเด็นซักถามเกี่ยวกับการทำสัญญาให้เก็บรักษาข้อมูลไว้เป็นความลับ
สามารถสอบถามได้ที่ เบอร์โทร 02-3788300

สัญญาให้เก็บรักษาข้อมูลไว้เป็นความลับ

สัญญาฉบับนี้ทำขึ้น เมื่อวันที่ ..... เดือน..... พ.ศ. .....
ณ.....
ตั้งอยู่เลขที่ ..... ระหว่าง
(ชื่อผู้ให้ข้อมูล)..... อยู่ที่ เลขที่ .....
เบอร์โทร.....ซึ่งในสัญญาฉบับนี้เรียกว่า **"ผู้ให้ข้อมูล"** ฝ่ายหนึ่ง และ
(ชื่อผู้รับข้อมูล) ..... อยู่ที่ เลขที่ .....
เบอร์โทร.....
ซึ่งในสัญญาฉบับนี้เรียกว่า **"ผู้รับข้อมูล"** อีกฝ่ายหนึ่ง
โดยที่ผู้ให้ข้อมูลเป็นผู้มีข้อมูลที่เกี่ยวข้องกับ*.....(องค์ความรู้ที่จะใช้ทำงานวิจัย/ผลงานวิจัย/ผลงานทรัพย์สินทางปัญญา เรื่อง)*..... ซึ่งต่อไปนี้จะเรียกว่า **"ข้อมูลที่เป็นความลับ"** และมีความประสงค์ที่จะเปิดเผยข้อมูลดังกล่าวให้แก่ผู้รับข้อมูล และผู้รับข้อมูลมีความต้องการที่จะใช้ข้อมูลเพื่อ.....*(นำข้อมูลนั้นไปพัฒนาต่อยอด/เพื่อนำไปประเมินความเป็นไปได้ในการร่วมทำวิจัย)* ทั้งสองฝ่ายจึงตกลงทำสัญญานี้ขึ้น โดยมีเงื่อนไขดังต่อไปนี้

1. ในสัญญานี้ "**ข้อมูลที่เป็นความลับ**" หมายความถึง ข้อมูลใดๆ รวมทั้งข้อมูลของบุคคลภายนอกที่ฝ่ายผู้ให้ข้อมูลได้เปิดเผยแก่ฝ่ายผู้รับข้อมูล และฝ่ายผู้ให้ข้อมูลประสงค์ให้ฝ่ายผู้รับข้อมูลเก็บรักษาข้อมูลดังกล่าวไว้เป็นความลับและ/หรือความลับทางการค้าของฝ่ายผู้ให้ข้อมูล โดยข้อมูลดังกล่าวจะเกี่ยวข้องกับองค์ความรู้ผลงานวิจัย ผลงานวิจัยของโครงการ และ/หรือการดำเนินงานโครงการ แผนและ/หรือแนวทางการวิจัย และ/หรือแผนทางการตลาด ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะกระบวนการ ขั้นตอนวิธี โปรแกรมคอมพิวเตอร์ (source code โปรแกรมปฏิบัติการ และฐานข้อมูลที่ใช้เชื่อมต่อโปรแกรมคอมพิวเตอร์) แบบ ต้นแบบ ภาพวาด สูตร เทคนิค การพัฒนาผลิตภัณฑ์ ข้อมูลการทดลอง และข้อมูลอื่นใดที่เกี่ยวข้องกับผลงานวิจัย ผลงานวิจัยของโครงการ และ/หรือการดำเนินงานโครงการ

2. การรักษาข้อมูลที่เป็นความลับ

2.1 ฝ่ายผู้รับข้อมูลตกลงว่าจะเก็บรักษาข้อมูลที่เป็นความลับที่ฝ่ายผู้ให้ข้อมูลได้เปิดเผยให้แก่ฝ่ายผู้รับข้อมูลภายใต้สัญญาฉบับนี้ โดยฝ่ายผู้รับข้อมูลตกลงที่จะดำเนินการเก็บรักษาข้อมูลที่เป็นความลับที่ได้รับจากฝ่ายผู้ให้ข้อมูลไว้เป็นความลับอย่างเคร่งครัด และไม่เปิดเผยข้อมูลที่เป็นความลับไม่ว่าทั้งหมดหรือแต่บางส่วนให้แก่บุคคลใดหรือองค์กรใดทราบ เว้นแต่จะเป็นการเปิดเผยข้อมูลที่เป็นความลับให้แก่ลูกจ้างหรือพนักงานของฝ่ายผู้รับข้อมูล หรือบุคคลภายนอกที่ต้องเกี่ยวข้องโดยตรงกับข้อมูลที่เป็นความลับนั้น และฝ่ายผู้รับข้อมูลจะต้องจัดให้ลูกจ้างหรือพนักงานของฝ่ายผู้รับข้อมูล หรือบุคคลภายนอกที่ต้องเกี่ยวข้องโดยตรงกับข้อมูลดังกล่าวได้ผูกพันและปฏิบัติตามเงื่อนไขในการรักษาข้อมูลที่เป็นความลับอย่างเคร่งครัดด้วย

2.2 หน้าที่ในการรักษาข้อมูลที่เป็นความลับตามสัญญาข้อ 2.1 จะไม่ใช้บังคับกับฝ่ายผู้รับข้อมูล ถ้าฝ่ายผู้รับข้อมูลสามารถแสดงพยานหลักฐานได้ว่า

(1) ข้อมูลดังกล่าวเป็นข้อมูลที่ฝ่ายผู้รับข้อมูลได้รับทราบอยู่ก่อนที่ฝ่ายผู้ให้ข้อมูลจะได้เปิดเผยข้อมูลนั้น

(2) ฝ่ายผู้รับข้อมูลได้รับข้อมูลที่เป็นความลับจากบุคคลที่สามที่ไม่อยู่ภายใต้ข้อกำหนดในเรื่องการรักษาความลับ หรือข้อจำกัดในเรื่องสิทธิ

(3) ข้อมูลดังกล่าวเป็นข้อมูลที่รู้กันโดยทั่วไปก่อนหรือขณะเวลาที่ฝ่ายผู้ให้ข้อมูลเปิดเผยข้อมูลที่เป็นความลับแก่ฝ่ายผู้รับข้อมูล หรือเป็นข้อมูลที่เป็นความลับที่ได้เปิดเผยต่อสาธารณะหลังจากที่ฝ่ายผู้ให้ข้อมูลได้เปิดเผยข้อมูลที่เป็นความลับให้แก่ฝ่ายผู้รับข้อมูล

(4) ข้อมูลดังกล่าวเป็นข้อมูลที่มาจากการพัฒนาโดยอิสระของฝ่ายผู้รับข้อมูลเอง

(5) ฝ่ายผู้รับข้อมูลได้รับความยินยอมเป็นหนังสือจากฝ่ายผู้ให้ข้อมูลก่อนเปิดเผยข้อมูลนั้น

2.3 การรักษาความลับตามสัญญานี้ ให้รักษาความลับตลอดระยะเวลาที่สัญญานี้มีผลบังคับใช้และมีผลต่อไปอีก 2 (สอง) ปีนับแต่วันที่สิ้นสุดสัญญา โดยฝ่ายผู้รับข้อมูลจะเปิดเผยข้อมูลที่เป็นความลับได้ต่อเมื่อได้รับความยินยอมเป็นหนังสือจากฝ่ายผู้ให้ข้อมูลดังกล่าวก่อน หรือจนกว่าข้อมูลที่เป็นความลับนั้นกลายเป็นข้อมูลที่ไม่ใช่ความลับโดยชอบด้วยกฎหมาย

3. ผู้รับข้อมูลตกลงใช้ข้อมูลที่เป็นความลับเพียงเพื่อให้บรรลุตามวัตถุประสงค์ที่กำหนดไว้ในสัญญานี้เท่านั้น

4. ผู้รับข้อมูลต้องไม่ทำซ้ำข้อมูลที่เป็นความลับแม้เพียงส่วนหนึ่งส่วนใดหรือทั้งหมด เว้นแต่การทำซ้ำเพื่อการใช้ข้อมูลที่เป็นความลับให้บรรลุผลตามวัตถุประสงค์ที่กำหนดไว้ในสัญญานี้ และไม่ทำวิศวกรรมย้อนกลับ หรือถอดรหัสข้อมูลที่เป็นความลับ ต้นแบบ หรือสิ่งอื่นใดที่บรรจุข้อมูลที่เป็นความลับ รวมทั้งไม่เคลื่อนย้าย พิมพ์ทับ หรือทำให้เสียรูปซึ่งสัญลักษณ์ที่แสดงเครื่องหมายสิทธิบัตร อนุสิทธิบัตร ลิขสิทธิ์ เครื่องหมายการค้า ตราสัญลักษณ์ และเครื่องหมายอื่นใดที่แสดงกรรมสิทธิ์ของต้นแบบหรือสำเนาของข้อมูลที่เป็นความลับที่ได้รับมาจากผู้ให้ข้อมูล

5. การชดใช้ค่าเสียหาย

กรณีที่ผู้รับข้อมูลฝ่าฝืนข้อกำหนดตามสัญญานี้ และก่อให้เกิดความเสียหายแก่ผู้ให้ข้อมูล ผู้รับข้อมูลจะต้องชดใช้ค่าเสียหายให้แก่ผู้ให้ข้อมูลและ/หรือบุคคลที่ได้รับความเสียหายสำหรับความเสียหายเช่นว่านั้น

6. สัญญานี้มีผลใช้บังคับตั้งแต่วันที่ทั้งสองฝ่ายลงนามเป็นต้นไป และมีกำหนดระยะเวลา 2 ปี นับแต่วันที่ลงนามในสัญญานี้ เมื่อสัญญานี้ได้สิ้นสุดลงไม่ว่ากรณีใดๆ ให้ข้อผูกพันในการเก็บความลับตามสัญญาฉบับนี้ยังคงมีผลใช้บังคับอยู่ต่อไปอีกเป็นเวลา 2 ปี (2+2 ปี)

7. สัญญาฉบับนี้ให้อยู่ใต้บังคับของกฎหมายประเทศไทย ให้ศาลของประเทศไทยมีอำนาจในกรณีที่มีข้อพิพาทใด ๆ อันเกิดขึ้นจากสัญญานี้

สัญญานี้ทำขึ้นสองฉบับมีข้อความถูกต้องตรงกัน คู่สัญญาได้อ่านและเข้าใจข้อความในสัญญานี้ละเอียดโดยตลอดแล้ว จึงได้ลงลายมือชื่อและประทับตราไว้ (หากมี) ไว้เป็นสำคัญต่อหน้าพยาน และคู่สัญญาต่างเก็บไว้ฝ่ายละฉบับ

ลงชื่อ.....ผู้ให้ข้อมูล
(.....)

ลงชื่อ.....ผู้รับข้อมูล
(.....)

ลงชื่อ.....พยา
(.....)

ชื่อ.....พยาน
(.....)

Logo คู่สัญญา

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล

โครงการ.....(ระบุชื่อบันทึกข้อตกลงความร่วมมือหรือสัญญาฉบับหลัก)....

ระหว่าง

สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) กับ.....(ชื่อคู่สัญญา).....

ข้อตกลงการประมวลผลข้อมูลส่วนบุคคล (“ข้อตกลง”) ฉบับนี้ทำขึ้น เมื่อวันที่.... (ระบุวันที่ลงนามในข้อตกลง)..... ณ สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน)

โดยที่ สถาบันพัฒนาองค์กรชุมชน (องค์การมหาชน) ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “พอช.” ฝ่ายหนึ่ง ได้ตกลงใน....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก).... ฉบับลงวันที่ ..... (ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก)..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “(บันทึกความร่วมมือ/สัญญา)” กับ ..... (ระบุชื่อคู่สัญญา)..... ซึ่งต่อไปในข้อตกลงฉบับนี้เรียกว่า “.....(ระบุชื่อเรียกคู่สัญญา.....” อีกฝ่ายหนึ่ง

ตาม (ระบุชื่อบันทึกความร่วมมือ/สัญญาหลัก) ดังกล่าวกำหนดให้ พอช. มีหน้าที่และความรับผิดชอบในส่วนของการ.....(ระบุขอบเขต สิทธิ หน้าที่ของ พอช. ตามบันทึกความร่วมมือ/สัญญาหลัก)..... ซึ่งในการดำเนินการดังกล่าวประกอบด้วยการมอบหมายหรือแต่งตั้งให้..... (ระบุชื่อคู่สัญญา).....เป็นผู้ดำเนินการกระบวนการเก็บรวบรวม ใช้ หรือเปิดเผย (“ประมวลผล”) ข้อมูลส่วนบุคคลแทนหรือในนามของ พอช.

พอช. ในฐานะผู้ควบคุมข้อมูลส่วนบุคคลเป็นผู้มีอำนาจตัดสินใจ กำหนดรูปแบบและกำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคล ได้.....(มอบหมาย/แต่งตั้ง/จ้าง/อื่น ๆ).....ให้..... (ระบุชื่อคู่สัญญา).....ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล ดำเนินการเพื่อวัตถุประสงค์ดังต่อไปนี้

๑. ..... (ระบุวัตถุประสงค์ที่ พอช. มอบหมายให้คู่สัญญาดำเนินการเกี่ยวกับข้อมูลส่วนบุคคล เช่น เพื่อการรับจ้างทำระบบยืนยันตัวตน เพื่อการรับทำ Survey เพื่อการลงทะเบียนผู้เข้าร่วมงานสัมมนา เพื่อการรับจ้างพิมพ์บัตรพนักงาน เพื่อการรับส่งเอกสาร เป็นต้น).....

๒. .....

โดยข้อมูลส่วนบุคคลที่ พอช. มอบหมาย.....(มอบหมาย/แต่งตั้ง/จ้าง/อื่น ๆ).....ให้.... (ระบุชื่อคู่สัญญา).....ประมวลผล ประกอบด้วย

๑. ..... (ระบุรายการข้อมูลส่วนบุคคลที่ พอช. มอบหมาย/เปิดเผยให้คู่สัญญาประมวลผล เช่น ชื่อ นามสกุลของเจ้าหน้าที่ เบอร์โทรศัพท์ ข้อมูลผู้ใช้งานแอปพลิเคชั่นทางรัฐ รายชื่อผู้เข้าร่วมงานสัมมนา เป็นต้น).....

๒. .....

ด้วยเหตุนี้ ทั้งสองฝ่ายจึงตกลงจัดทำข้อตกลงฉบับนี้ และให้ถือข้อตกลงฉบับนี้เป็นส่วนหนึ่ง....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....เพื่อเป็นหลักฐานการควบคุมดูแลการประมวลผลข้อมูลส่วนบุคคลที่ พอช. มอบหมายหรือแต่งตั้งให้..... (ระบุชื่อคู่สัญญา)..... ดำเนินการ อันเนื่องมาจากการดำเนินการตามหน้าที่และความรับผิดชอบตาม....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....ฉบับลงวันที่ ..... (ระบุวันที่ลงนามข้อตกลงความร่วมมือหรือวันทำสัญญาหลัก)..... และเพื่อดำเนินการให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และกฎหมายอื่น ๆ ที่ออกตามความในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ซึ่งต่อไปในข้อตกลงฉบับนี้ รวมเรียกว่า “กฎหมายคุ้มครองข้อมูลส่วนบุคคล” ทั้งที่มีผลใช้บังคับอยู่ ณ วันทำข้อตกลงฉบับนี้และที่จะมีการเพิ่มเติมหรือแก้ไขเปลี่ยนแปลงในภายหลัง โดยมีรายละเอียดดังนี้

๑. ..... (ระบุชื่อคู่สัญญา)..... รับทราบว่า ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลธรรมดาซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม โดย..... (ระบุชื่อคู่สัญญา)..... จะดำเนินการตามที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลกำหนด เพื่อคุ้มครองให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสมและถูกต้องตามกฎหมาย

โดยในการดำเนินการตามข้อตกลงนี้ ..... (ระบุชื่อคู่สัญญา).....จะประมวลผลข้อมูลส่วนบุคคลเมื่อได้รับคำสั่งที่เป็นลายลักษณ์อักษรจาก พอช. แล้วเท่านั้น ทั้งนี้ เพื่อให้ปราศจากข้อสงสัย การดำเนินการประมวลผลข้อมูลส่วนบุคคลโดย..... (ระบุชื่อคู่สัญญา).....ตามหน้าที่และความรับผิดชอบตาม....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....ถือเป็นการได้รับคำสั่งที่เป็นลายลักษณ์อักษรจาก พอช. แล้ว

๒. ..... (ระบุชื่อคู่สัญญา).....จะกำหนดให้การเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้ถูกจำกัดเฉพาะเจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ได้รับมอบหมาย มีหน้าที่เกี่ยวข้องหรือมีความจำเป็นในการเข้าถึงข้อมูลส่วนบุคคลภายใต้ข้อตกลงฉบับนี้เท่านั้น และจะดำเนินการเพื่อให้พนักงานและ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ได้รับมอบหมายจาก..... (ระบุชื่อคู่สัญญา).....ทำการประมวลผลและรักษาความลับของข้อมูลส่วนบุคคลด้วยมาตรฐานเดียวกัน

๓. ..... (ระบุชื่อคู่สัญญา).....จะควบคุมดูแลให้เจ้าหน้าที่ และ/หรือลูกจ้าง ตัวแทนหรือบุคคลใด ๆ ที่ปฏิบัติหน้าที่ในการประมวลผลข้อมูลส่วนบุคคล ปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัด และดำเนินการประมวลผลข้อมูลส่วนบุคคลตามวัตถุประสงค์ของการดำเนินการตามข้อตกลงฉบับนี้เท่านั้น โดยจะไม่ทำซ้ำ คัดลอก ทำสำเนา บันทึกภาพข้อมูลส่วนบุคคลไม่ว่าทั้งหมดหรือแต่บางส่วนเป็นอันขาด เว้นแต่

เป็นไปตามเงื่อนไขของบันทึกความร่วมมือหรือสัญญา หรือกฎหมายที่เกี่ยวข้องจะระบุหรือบัญญัติไว้เป็นประการอื่น

๔. ..... (ระบุชื่อคู่สัญญา).....จะดำเนินการเพื่อช่วยเหลือหรือสนับสนุน พอช. ในการตอบสนองต่อคำร้องที่เจ้าของข้อมูลส่วนบุคคลแจ้งต่อ พอช. อันเป็นการใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลในส่วนที่เกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลในขอบเขตของข้อตกลงฉบับนี้

อย่างไรก็ดี ในกรณีที่เจ้าของข้อมูลส่วนบุคคลยื่นคำร้องขอใช้สิทธิดังกล่าวต่อ..... (ระบุชื่อคู่สัญญา).....โดยตรง ..... (ระบุชื่อคู่สัญญา).....จะดำเนินการแจ้งและส่งคำร้องดังกล่าวให้แก่ พอช. ทันที โดย..... (ระบุชื่อคู่สัญญา).....จะไม่เป็นผู้ตอบสนองต่อคำร้องดังกล่าว เว้นแต่ พอช. จะได้มอบหมายให้..... (ระบุชื่อคู่สัญญา).....ดำเนินการเฉพาะเรื่องที่เกี่ยวข้องกับคำร้องดังกล่าว

๕. ..... (ระบุชื่อคู่สัญญา).....จะจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (Record of Processing) ทั้งหมดที่..... (ระบุชื่อคู่สัญญา).....ประมวลผลในขอบเขตของข้อตกลงฉบับนี้ และจะดำเนินการส่งมอบบันทึกรายการดังกล่าวให้แก่ พอช. ทุก.....(ระบุความถี่ของการส่งมอบบันทึกรายการ เช่น ทุกสัปดาห์หรือทุกเดือน).... และ/หรือทันทีที่ พอช. ร้องขอ

๖. ..... (ระบุชื่อคู่สัญญา).....จะจัดให้มีและคงไว้ซึ่งมาตรการรักษาความปลอดภัยสำหรับการประมวลผลข้อมูลที่มีความเหมาะสมทั้งในเชิงองค์กรและเชิงเทคนิคตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลได้ประกาศกำหนดและ/หรือตามมาตรฐานสากล โดยคำนึงถึงลักษณะ ขอบเขต และวัตถุประสงค์ของการประมวลผลข้อมูลตามที่กำหนดในข้อตกลงฉบับนี้เป็นสำคัญ เพื่อคุ้มครองข้อมูลส่วนบุคคลจากความเสี่ยงอันเกี่ยวเนื่องกับการประมวลผลข้อมูลส่วนบุคคล เช่น ความเสียหายอันเกิดจากการละเมิด อุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย เป็นต้น

๗. เว้นแต่กฎหมายที่เกี่ยวข้องจะบัญญัติไว้เป็นประการอื่น ..... (ระบุชื่อคู่สัญญา).....จะทำการลบหรือทำลายข้อมูลส่วนบุคคลที่ทำการประมวลผลภายใต้ข้อตกลงฉบับนี้ภายใน....(ระบุจำนวนวันที่จะทำการลบทำลายข้อมูล).....วัน นับแต่วันที่ดำเนินการประมวลผลเสร็จสิ้น หรือวันที่ พอช. และ ..... (ระบุชื่อคู่สัญญา).....ได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิก....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก).... แล้วแต่กรณีใดจะเกิดขึ้นก่อน

นอกจากนี้ ในกรณีปรากฏว่า..... (ระบุชื่อคู่สัญญา).....หมดความจำเป็นจะต้องเก็บรักษาข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ก่อนสิ้นระยะเวลาตามวรรคหนึ่ง ..... (ระบุชื่อคู่สัญญา).....จะทำการลบหรือทำลายข้อมูลส่วนบุคคลตามข้อตกลงฉบับนี้ทันที

๘. กรณีที่..... (ระบุชื่อคู่สัญญา).....พบพฤติการณ์ใด ๆ ที่มีลักษณะที่กระทบต่อการรักษาความปลอดภัยของข้อมูลส่วนบุคคลที่..... (ระบุชื่อคู่สัญญา).....ประมวลผลภายใต้ข้อตกลงฉบับนี้ ซึ่งอาจก่อให้เกิดความเสียหายจากการละเมิด อุบัติเหตุ การลบ ทำลาย สูญหาย เปลี่ยนแปลง แก้ไข เข้าถึง ใช้

เปิดเผยหรือโอนข้อมูลส่วนบุคคลโดยไม่ชอบด้วยกฎหมาย แล้ว..... (ระบุชื่อคู่สัญญา).....จะดำเนินการแจ้งให้ พอช. ทราบโดยทันทีภายในเวลาไม่เกิน 24 ชั่วโมง

๙. การแจ้งถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้นภายใต้ข้อตกลงนี้..... (ระบุชื่อคู่สัญญา)..... จะใช้มาตรการตามที่เห็นสมควรในการระบุถึงสาเหตุของการละเมิด และป้องกันปัญหาดังกล่าวมิให้เกิดซ้ำ และจะให้ข้อมูลแก่ พอช. ภายใต้ขอบเขตที่กฎหมายคุ้มครองข้อมูลส่วนบุคคลได้กำหนด ดังต่อไปนี้

- รายละเอียดของลักษณะและผลกระทบที่อาจเกิดขึ้นของการละเมิด
- มาตรการที่ถูกใช้เพื่อลดผลกระทบของการละเมิด
- ประเภทของข้อมูลส่วนบุคคลและเจ้าของข้อมูลส่วนบุคคลที่ถูกละเมิด หากมีปรากฏ
- ข้อมูลอื่น ๆ เกี่ยวข้องกับการละเมิด

๑๐. หน้าที่และความรับผิดของ..... (ระบุชื่อคู่สัญญา).....ในการปฏิบัติตามข้อตกลงจะสิ้นสุดลงนับแต่วันที่ปฏิบัติงานที่ตกลงเสร็จสิ้น หรือ วันที่..... (ระบุชื่อคู่สัญญา).....และ พอช. ได้ตกลงเป็นลายลักษณ์อักษรให้ยกเลิก....(ระบุชื่อบันทึกข้อตกลงความร่วมมือ/สัญญาหลัก)....แล้วแต่กรณีใดจะเกิดขึ้นก่อน อย่างไรก็ดี การสิ้นผลลงของข้อตกลงนี้ ไม่กระทบต่อหน้าที่ของ..... (ระบุชื่อคู่สัญญา).....ในการลบหรือทำลายข้อมูลส่วนบุคคลตามที่ได้กำหนดในข้อ 7 ของข้อตกลงฉบับนี้

ทั้งสองฝ่ายได้อ่านและเข้าใจข้อความโดยละเอียดตลอดแล้ว เพื่อเป็นหลักฐานแห่งการนี้ ทั้งสองฝ่ายจึงได้ลงนามไว้เป็นหลักฐานต่อหน้าพยาน ณ วัน เดือน ปี ที่ระบุข้างต้น

ลงชื่อ	ลงชื่อ .....
(.....)	(.....)
.....	.....
ลงชื่อ ..... พยาน	ลงชื่อ ..... พยาน
(.....)	(.....)
.....	.....