สารบัญ

สารบัญ

๕. นโยบายการลงทะเบียนผู้ใช้

- แบบคำขอสำหรับลงทะเบียนผู้ใช้

๖. นโยบายการบริหารจัดการช่องโหว่ของระบบ

๗. นโยบายการจัดการกับโปรแกรมไม่ประสงค์ดี

๘. นโยบายการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย

ขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี

ขั้นตอนปฏิบัติสำหรับการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย

- แบบรายงานเหตุการณ์ทางด้านความมั่นคงปลอดภัย

9.นโยบายการจัดการความมั่นคงปลอดภัยสำหรับระบบและเครือข่าย

นโยบายควบคุมการเข้าถึง

ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ

ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ

๓๘. โครงสร้างพื้นฐานสารสนเทศที่ควบคุม

๓๙.แบบคำขอสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ

โครงสร้างพื้นฐานสารสนเทศที่ควบคุม

10. นโยบายการจัดการทรัพยากรของระบบ

11. นโยบายการแลกเปลี่ยนสารสนเทศระหว่างสำนักงาน

12. นโยบายการสำรองและทดสอบกู้คืนข้อมูล

- แนวทางปฏิบัติ สำหรับการสำรองและทดสอบกู้คืนข้อมูล

- แนวทางปฏิบัติ สำหรับการสำรองและทดสอบกู้คืนข้อมูล

13.นโยบายการสร้างความมั่นคงปลอดภัยทางกายภาพสำหรับพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย

14. นโยบายการป้องกันภัยคุกคามทางด้านสิ่งแวดล้อม

15. นโยบายการป้องกันระบบ อุปกรณ์และสายสัญญาณต่าง ๆ

16. นโยบายการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์(Log) และการดำเนินการแก้ไข

17. นโยบายการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550

18. นโยบายการกู้คืนระบบ

ส่วนที่ 4 นโยบายการจัดการด้านบุคลากร สำหรับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

1. นโยบายการจัดการด้านบุคลากร

ส่วนที่ 5 นโยบายการเผยแพร่ข้อมูลสู่สาธารณะ

สำหรับผู้เป็นเจ้าของหรือรับผิดชอบต่อข้อมูลที่ต้องทำการเผยแพร่สู่สาธารณะ

1. นโยบายการนำข้อมูลเผยแพร่สู่สาธารณะ

ส่วนที่ 1 นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร

ส่วนที่ 2 นโยบายการใช้งานระบบคอมพิวเตอร์และเครือข่ายสำหรับผู้ใช้งาน

นโยบายการใช้งานระบบคอมพิวเตอร์และเครือข่ายประกอบด้วย

๔๐. นโยบายการป้องกันทรัพย์สินของสำนักงาน

๔๑. นโยบายการป้องกันไวรัสบนเครื่องคอมพิวเตอร์

๔๒. นโยบายการห้ามการติดตั้งระบบหรืออุปกรณ์ต่าง ๆ เพิ่มเติม

๔๓. นโยบายการใช้งานอินเตอร์เน็ต

๔๔. นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)

๔๕. นโยบายการป้องกันการใช้ทรัพยากรผิดวัตถุประสงค์

๔๖. นโยบายการใช้งานเครื่องคอมพิวเตอร์โน้ตบุ๊ค

๔๗. นโยบายการกำหนดและป้องกันรหัสผ่าน

๔๘. นโยบายการเข้าไปปฏิบัติงานในห้องเครื่องคอมพิวเตอร์แม่ข่ายหลัก

๔๙. นโยบายการจัดการเอกสารลับบนกระดาษ หรือบนสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

๕๐. นโยบายการทำลายข้อมูลบนสื่อบันทึกข้อมูล

๕๑. นโยบายการลงทะเบียนการใช้งานระบบสารสนเทศ

แบบฟอร์มการขอใช้บริการระบบสารสนเทศ

๕๒. นโยบายการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัย

ส่วนที่ 3 นโยบายการจัดการคอมพิวเตอร์และเครือข่ายสำหรับเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ

๙. นโยบายการจัดทำคู่มือการปฏิบัติงาน

๑๐. นโยบายการตรวจสอบข้อมูลความรู้เกี่ยวข้องกับผลิตภัณฑ์ที่สำนักงานใช้งานและความรู้ที่เกี่ยวกับความมั่นคงปลอดภัย

๑๑. นโยบายการพัฒนาระบบงาน

แนวทางปฏิบัติในการตรวจสอบข้อมูลนำเข้า

แนวทางปฏิบัติในการตรวจสอบความถูกต้องของการประมวลผลข้อมูล

มาตรฐานทางด้านความมั่นคงปลอดภัยในการพัฒนาระบบงาน

ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบงาน

แบบคำขออนุมัติดำเนินการเปลี่ยนแปลงระบบงาน

แนวทางปฏิบัติในการตรวจข้อมูลนำเข้า

แนวทางปฏิบัติในการตรวจสอบความถูกต้องของการประมวลผลข้อมูล

มาตรฐานทางด้านความมั่นคงปลอดภัยในการพัฒนาระบบงาน

4. นโยบายความคุมการติดตั้งบนระบบให้บริการจริง

๑๒. นโยบายการลงทะเบียนผู้ใช้

- แบบคำขอสำหรับลงทะเบียนผู้ใช้

๑๓.นโยบายการบริหารจัดการช่องโหว่ของระบบ

๑๔.นโยบายการจัดการกับโปรแกรมไม่ประสงค์ดี

๑๕.นโยบายการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย

ขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี

ขั้นตอนปฏิบัติสำหรับการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย

- แบบรายงานเหตุการณ์ทางด้านความมั่นคงปลอดภัย

9.นโยบายการจัดการความมั่นคงปลอดภัยสำหรับระบบและเครือข่าย

นโยบายควบคุมการเข้าถึง

ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ

ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ

๕๓. โครงสร้างพื้นฐานสารสนเทศที่ควบคุม

๕๔. แบบคำขอสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ

โครงสร้างพื้นฐานสารสนเทศที่ควบคุม

10. นโยบายการจัดการทรัพยากรของระบบ

11. นโยบายการแลกเปลี่ยนสารสนเทศระหว่างสำนักงาน

12. นโยบายการสำรองและทดสอบกู้คืนข้อมูล

- แนวทางปฏิบัติ สำหรับการสำรองและทดสอบกู้คืนข้อมูล

- แนวทางปฏิบัติ สำหรับการสำรองและทดสอบกู้คืนข้อมูล

13.นโยบายการสร้างความมั่นคงปลอดภัยทางกายภาพสำหรับพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย

14. นโยบายการป้องกันภัยคุกคามทางด้านสิ่งแวดล้อม

15. นโยบายการป้องกันระบบ อุปกรณ์และสายสัญญาณต่าง ๆ

16. นโยบายการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์(Log) และการดำเนินการแก้ไข

17. นโยบายการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550

18. นโยบายการกู้คืนระบบ

ส่วนที่ 4 นโยบายการจัดการด้านบุคลากร สำหรับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

2. นโยบายการจัดการด้านบุคลากร

ส่วนที่ 5 นโยบายการเผยแพร่ข้อมูลสู่สาธารณะ

สำหรับผู้เป็นเจ้าของหรือรับผิดชอบต่อข้อมูลที่ต้องทำการเผยแพร่สู่สาธารณะ

1. นโยบายการนำข้อมูลเผยแพร่สู่สาธารณะ

นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ
ของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์
(OPS ICT Security Policy)

๑. หลักการและเหตุผล

๑. ตามที่ได้มีการประกาศใช้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ ซึ่งมีผลกระทบต่อสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ซึ่งเป็นผู้ให้บริการระบบเครือข่ายสาธารณะ (Internet) และผู้ใช้งานระบบคอมพิวเตอร์เครือข่าย ซึ่งจะต้องมีการใช้งานระบบคอมพิวเตอร์เครือข่ายอย่างระมัดระวัง เพราะอาจจะก่อให้เกิดความเสียหายทั้งผู้ใช้งานและองค์กร รวมถึงอาจจะผิดต่อกฎหมายดังกล่าว

๒. ด้วยแนวทางการพัฒนาคุณภาพการบริหารจัดการภาครัฐ (PMQA) หมวด ๔ การวัด การวิเคราะห์ และการจัดการความรู้ เพื่อให้การปฏิบัติงานระบบเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ มีความเหมาะสม มีประสิทธิภาพและมีความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศอย่างครบถ้วน รวมถึงการดำเนินการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ภายใต้แนวทางการดำเนินงานบริหารจัดการบ้านเมืองที่ดี และเพื่อเป็นการเตรียมความพร้อมการดำเนินงานภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้การดำเนินงานเป็นไปตามกฎหมายและแนวทางการดำเนินงานดังกล่าวข้างต้น สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ จึงได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นเครื่องมือที่สำคัญในการปฏิบัติงานราชการและการบริหารงานราชการ ดังต่อไปนี้

๒. วัตถุประสงค์และขอบเขต

สำนักงานปลัดกระทรวงเกษตรและสหกรณ์ (สำนักงาน) ได้นำระบบเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานทั้งในด้านการบริหารงานภายในสำนักงานและการบริการผู้ใช้ระบบเครือข่ายคอมพิวเตอร์ และเพื่อให้การใช้งานระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย สามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ จึงได้กำหนดนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ครอบคลุมถึงประเด็นสำคัญ ดังนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การมีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและมีแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการตามวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้อย่างปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๓. องค์ประกอบของนโยบาย

องค์ประกอบของนโยบายการรักษาความมั่นปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงาน ใช้แนวทางและกระบวนการโดยอ้างอิงตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑:๒๐๐๕ และ ISO/IEC ๑๗๗๙๙:๒๐๐๕ และมาตรฐานการรักษาความมั่นปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) ของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ โดยแบ่งออกเป็น ๕ ส่วน ตามเอกสารแนบท้ายนโยบายนี้ ดังต่อไปนี้

ส่วนที่ ๑ นโยบายการบริหารจัดการความมั่นคงปลอดภัย สำหรับผู้บริหาร

ส่วนที่ ๒ นโยบายการใช้งานคอมพิวเตอร์และเครือข่าย สำหรับผู้ใช้

ส่วนที่ ๓ นโยบายการจัดการคอมพิวเตอร์และเครือข่าย สำหรับเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ

ส่วนที่ ๔ นโยบายการจัดการด้านบุคลากร สำหรับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๕ นโยบายการเผยแพร่ข้อมูลสู่สาธารณะ สำหรับผู้เป็นเจ้าของหรือรับผิดชอบต่อข้อมูลที่ต้องการเผยแพร่สู่สาธารณะ

องค์ประกอบนโยบายในแต่ละส่วนที่กล่าวมาข้างต้นจะประกอบด้วย วัตถุประสงค์ ผู้รับผิดชอบ อ้างอิงมาตรฐานและการดำเนินการ รวมถึงมาตรฐาน ขั้นตอนปฏิบัติและแนวทางปฏิบัติที่เกี่ยวข้องในการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงาน เพื่อที่จะทำให้สำนักงานมีมาตรการในการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระบบที่ปลอดภัย ช่วยลดความเสียหายจากการดำเนินงานที่จะเกิดกับทรัพย์สินและบุคลากรของสำนักงาน และทำให้สำนักงานสามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศฉบับนี้ จัดเป็นมาตรฐานด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน ซึ่งข้าราชการ ลูกจ้างประจำและพนักงานราชการของสำนักงาน รวมทั้งหน่วยงานภายนอกที่เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ กันยายน พ.ศ. ๒๕๕๓

(นายยุคล ลิ้มแหลมทอง)
ปลัดกระทรวงเกษตรและสหกรณ์

คำนิยาม

คำนิยามที่ใช้ประกาศประกอบด้วย

“กระทรวง” หมายถึง กระทรวงเกษตรและสหกรณ์

“สำนักงาน” หมายถึง สำนักงานปลัดกระทรวงเกษตรและสหกรณ์

“หน่วยงาน” หมายถึง สำนักงาน กอง ศูนย์และกลุ่ม รวมถึงหน่วยงานย่อยต่าง ๆ ในสังกัดสำนักงานหรือหน่วยงานที่ใช้งานสถานที่อยู่ในอาคารสำนักงาน ณ ถนนราชดำเนินนอก

“ศูนย์” หมายถึง ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

“ผู้บริหารสูงสุด” หมายถึง ปลัดกระทรวงเกษตรและสหกรณ์

“ผู้บริหารเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO)” หมายถึง ผู้บริหารเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ รองปลัดกระทรวงเกษตรและสหกรณ์ผู้ที่มีหน้าที่และความรับผิดชอบในการบริหารงานเทคโนโลยีสารสนเทศของสำนักงาน การจัดทำแผนแม่บทและแผนปฏิบัติการด้านเทคโนโลยีสารสนเทศของสำนักงาน การจัดทำนโยบายและกำกับดูแลการดำเนินการด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ กำกับดูแลการดำเนินการตามนโยบายเทคโนโลยีสารสนเทศแห่งชาติและติดตามผลการดำเนินงานตามนโยบาย กำกับดูแลการพัฒนาเทคโนโลยีสารสนเทศให้เป็นไปตามมาตรฐานที่กำหนดและพัฒนาการใช้ให้มีประสิทธิภาพเกิดประโยชน์สูงสุดและคุ้มค่า กำกับดูแลติดตามและประเมินผล และการรายงานผลการปฏิบัติงานสารสนเทศ

“ผู้บังคับบัญชา” หมายถึง ผู้บังคับบัญชาระดับสำนัก/กอง/กลุ่มหรือระดับกรมทั้งบุคคลที่ได้รับมอบหมาย

“ผู้ใช้งาน” หมายถึง ข้าราชการ ลูกจ้างและพนักงานราชการหรือผู้ที่สำนักงานอนุญาต (Authorized Users) ให้สามารถเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน

“การรักษาความมั่นคงปลอดภัย” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน

“มาตรฐาน” หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

“ขั้นตอนปฏิบัติ” หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

“แนวทางปฏิบัติ” หมายถึง แนวทางที่ควรปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายได้ง่ายขึ้น

“ระบบเทคโนโลยีสารสนเทศ (Information Technology System)” หมายถึง ระบบงานของสำนักงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สำนักงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

“เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ” หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้สามารถเข้าใช้งานดูแลรักษาระบบเทคโนโลยีสารสนเทศของสำนักงาน ดังนี้

- ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่ายคอมพิวเตอร์
- ผู้พัฒนาระบบ (System Developer) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่ในการพัฒนาและดูแลรักษาระบบงานสารสนเทศของหน่วยงาน

“หน่วยงานภายนอก” หมายถึง หน่วยงานที่สำนักงานอนุญาตให้มีสิทธิในการเข้าถึงหรือใช้ข้อมูล หรือทรัพย์ชนิดต่างๆ ของสำนักงาน โดยจะได้รับสิทธิในการใช้ระบบตามประเภทงาน และต้องรับผิดชอบในการรักษาความลับด้วย

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

“ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data)” หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“สารสนเทศ (Information)” หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

“ระบบคอมพิวเตอร์ (Computer System)” หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยมีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวทางการปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบเครือข่าย (Network System)” หมายถึง ระบบที่ใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของสำนักงาน ได้แก่ ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเตอร์เน็ต (Internet) เป็นต้น

- ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานของ สำนักงานเข้าด้วยกันเป็นเครือข่ายทีมีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูล และสารสนเทศภายในหน่วยงาน
- ระบบอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของสำนักงาน เข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

“ห้องคอมพิวเตอร์แม่ข่ายกลาง (Server Room) ” หมายถึง ห้องที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายหรือคอมพิวเตอร์หลัก และอุปกรณ์เครือข่ายหลักที่ใช้งานในสำนักงาน

“จดหมายอิเล็กทรอนิกส์ (E-mail)” หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคนก็ได้ โดยข่าวสารที่ส่งนั้นจะถูกเก็บไว้ในตู้จดหมาย (Mail Box) ที่กำหนดไว้สำหรับผู้ใช้เครือข่าย ผู้รับสามารถเปิดอ่านข่าวสารหรือพิมพ์ลงกระดาษหรือจะลบทิ้งก็ได้

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

“เจ้าของข้อมูล” หมายถึง หน่วยงานที่รับผิดชอบในการนำข้อมูลของสำนักงานเข้าในระบบเทคโนโลยีสารสนเทศ โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ และได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

“ทรัพย์สิน” หมายถึง ทรัพย์สินด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟแวร์ที่มีค่าลิขสิทธิ์ เป็นต้น

“รหัสผ่าน (Password)” หมายถึง ตัวอักษร หรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“โปรแกรมไม่ประสงค์” หมายถึง โปรแกรมที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือโปรแกรมอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ทำให้ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

“ระบบเครือข่ายไร้สาย (Wireless) หมายถึง ระบบเครือข่ายสื่อสารข้อมูล โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ ”

“MAC Address (Media Access Control Address)” หมายถึง หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่มีต่อระบบเครือข่าย หมายเลขนี้จะมากับอีเธอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

“WEP (Wired Equivalent Privacy)” หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าตัวเลขนี้

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

ส่วนที่ ๑
นโยบายการบริหารจัดการความมั่นคงปลอดภัยสำหรับผู้บริหาร

วัตถุประสงค์

เพื่อให้มีการบริหารจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของสำนักงาน เพื่อให้สอดคล้องกับมาตรฐานสากล ISO/IEC ๒๗๐๐๑

ผู้รับผิดชอบ

ผู้บริหารเทคโนโลยีสารสนเทศของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ (CIO)

อ้างอิงมาตรฐาน

- หมวดที่ ๑ นโยบายความมั่นคงปลอดภัย
- หมวดที่ ๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับสำนักงาน
- หมวดที่ ๓ การบริหารจัดการทรัพย์สินของสำนักงาน
- หมวดที่ ๔ ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร
- หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
- หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน
- หมวดที่ ๗ การควบคุมการเข้าถึง
- หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ
- หมวดที่ ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสำนักงาน
- หมวดที่ ๑๐ การบริหารความต่อเนื่องในการดำเนินงานของสำนักงาน
- หมวดที่ ๑๑ การปฏิบัติตามข้อกฎหมาย

การดำเนินการ

๑. จัดให้มีการทำและทบทวนหรือปรับปรุงนโยบายความมั่นคงปลอดภัยและนโยบายสนับสนุนต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อสำนักงาน

๒. จัดให้มีการทำหนังสือเวียนปีละ ๑ ครั้งเพื่อแจ้งให้เจ้าหน้าที่ทั้งหมดของสำนักงานได้รับทราบเกี่ยวกับประเภทของเหตุการณ์ด้านความมั่นคงปลอดภัยที่ต้องทำการรายงาน และข้อมูลที่ต้องทำรายงาน รวมทั้งให้ปรับปรุงข้อมูลการรายงานดังกล่าวตามความจำเป็น ประเภทของเหตุการณ์ที่ต้องรายงาน ได้แก่ การกระทำที่ผิดต่อ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เหตุการณ์อื่นๆ ที่เป็นการละเมิดนโยบายด้านความมั่นคงปลอดภัย

๓. จัดให้มีทรัพยากรด้านบุคลากร งบประมาณ การบริหารจัดการ และวัตถุดิบที่เพียงพอต่อการบริหารจัดการด้านความมั่งคงปลอดภัยในแต่ละปีงบประมาณ ซึ่งรวมถึงแผนความมั่นคงปลอดภัยสารสนเทศที่จะดำเนินการในปีงบประมาณนั้นด้วย

๔. จัดการให้มีการเพิ่มทักษะด้านระบบความมั่นคงปลอดภัย เป็นระยะๆ สำหรับเจ้าหน้าที่เทคโนโลยีสารสนเทศ เพื่อใช้ในการสนับสนุนการปฏิบัติงาน และการวางแผนการอบรมเพิ่มพูนความรู้ความสามารถของเจ้าหน้าที่

๕. จัดให้มีการอบรมเจ้าหน้าที่เพื่อสร้างความตระหนักที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๖. จัดให้มีการซ้อมแผนกู้คืนระบบอย่างน้อยปีละ ๑ ครั้ง และปรับปรุงแผนฯ ตามความเหมาะสม รวมทั้งจัดให้มีการจัดทำแผนเพื่อปรับปรุงหรือแก้ไขปัญหาที่พบ

๗. จัดให้มีการกำหนดบริการใดที่อนุญาตให้ใช้งาน และบริการใดไม่อนุญาตให้ใช้งานบนระบบเครือข่าย รวมทั้งปรับปรุงรายชื่อบริการดังกล่าวตามความจำเป็น และจัดให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารดำเนินการเพื่อให้เป็นไปตามนโยบายที่กำหนดไว้

๘. จัดให้มีเจ้าหน้าที่ดำเนินงานด้านความมั่นคงปลอดภัยสำหรับสารสนเทศและกำหนดหน้าที่ความรับผิดชอบ รวมทั้งปรับปรุงโครงสร้างดังกล่าวตามความจำเป็น

๙. แสดงเจตนารมณ์หรือสื่อสารอย่างสม่ำเสมอเพื่อให้เจ้าหน้าที่ทั้งหมดได้เห็นถึงความสำคัญของการปฏิบัติตามนโยบายความมั่นคงปลอดภัยและสนับสนุนต่างๆ โดยเคร่งครัด

ส่วนที่ ๒
นโยบายการใช้งานระบบคอมพิวเตอร์และเครือข่าย
สำหรับผู้ใช้งาน

ผู้ใช้งานมีหน้าที่รับผิดชอบต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงาน ดังนี้

- ประพฤติและปฏิบัติตามนโยบายความมั่นคงปลอดภัยโดยเคร่งครัด
- ปฏิบัติตามกิจกรรมหรือกระบวนการด้านความมั่นคงปลอดภัยที่กำหนดไว้
- ไม่เข้าถึง เปิดเผย เปลี่ยนแปลง แก้ไข ทำลาย หรือทำให้เสียหายต่อทรัพย์สินสารสนเทศของสำนักงานโดยไม่ได้รับอนุญาต
- ไม่รบกวนหรือแทรกแซงการสื่อสารของผู้อื่นจนทำให้ไม่สามารถดำเนินต่อไปได้
- ปฏิบัติงานตามหน้าที่ความรับผิดชอบของตนเองที่ได้กำหนดไว้
- รายงานเหตุการณ์ความเสี่ยง จุดอ่อน หรือเหตุการณ์ความมั่นคงปลอดภัยที่พบไปยังศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือหน่วยงานอื่นๆ ที่เกี่ยวข้อง
- ในกรณีที่มีการละเลยต่อหน้าที่หรือนโยบายที่กำหนดไว้ จะมีการสอบสวนและดำเนินการทั้งทางวินัยและกฎหมายตามความเหมาะสม

นโยบายการใช้งานระบบคอมพิวเตอร์และเครือข่าย ประกอบด้วย

๑. นโยบายการป้องกันทรัพย์สินของสำนักงาน

วัตถุประสงค์

๑. เพื่อป้องกันทรัพย์สินของสำนักงานจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต สูญหาย เสียหาย หรือถูกขโมย

๒. เพื่อให้มีการใช้งานเครื่องคอมพิวเตอร์ที่สำนักงานจัดไว้ให้อย่างเหมาะสม และป้องกันการสูญหาย เสียหาย หรือถูกเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

ผู้ใช้งาน

อ้างอิงมาตรฐาน

หมวดที่ ๓ การบริหารจัดการทรัพย์สินของสำนักงาน

หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

หมวดที่ ๗ การควบคุมการเข้าถึง

การดำเนินการ

๑. ตรวจสอบว่าเครื่องคอมพิวเตอร์ของสำนักงานได้รับการติดตั้งโปรแกรมตามรายชื่อโปรแกรมมาตรฐานที่กำหนดให้ติดตั้งหรือไม่ (โปรแกรมดังกล่าว ได้แก่ โปรแกรมออฟฟิส โปรแกรมป้องกันไวรัส หรือโปรแกรมอื่น ๆ เป็นต้น) หากพบว่ายังไม่ได้ติดตั้ง ให้ติดต่อผู้ดูแลระบบที่เกี่ยวข้องเพื่อขอรับการติดตั้งก่อนการใช้งาน

๒. ออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

๓. ปิดเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อไม่มีการใช้งานเกิน ๑ ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเซิร์ฟเวอร์ให้บริการที่ต้องใช้งานตลอด ๒๔ ชั่วโมง

๔. การตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานหรือถือครองให้มีการล็อค (Lock) หน้าจอโดยอัตโนมัติหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที

๕. ให้ขออนุมัติจากผู้บังคับบัญชา ในกรณีที่ต้องการนำอุปกรณ์คอมพิวเตอร์ต่างๆ ออกนอกสำนักงาน

๖. ระมัดระวังและดูแลทรัพย์สินของสำนักงานที่ตนเองใช้งานหรือถือครองเสมือนเป็นทรัพย์สินของตนเอง หากเกิดความสูญหายโดยประมาทเลินเล่อต้องรับผิดชอบหรือชดใช้ต่อความเสียหายนั้น

๒. นโยบายการป้องกันไวรัสบนเครื่องคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อป้องกันข้อมูลในเครื่องคอมพิวเตอร์ไม่ให้เกิดความเสียหาย

๒ เพื่อให้เครื่องคอมพิวเตอร์ทำงานอย่างถูกต้อง มีเสถียรภาพ เชื่อถือได้ และปลอดภัยจากการถูกบุกรุกหรือโจมตี

ผู้รับผิดชอบ

ผู้ใช้งาน

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

การดำเนินการ

ตรวจสอบการทำงานของโปรแกรมป้องกันไวรัสว่ายังทำงานได้ตามปกติหรือไม่ และมีการปรับปรุงฐานข้อมูลไวรัสอย่างสม่ำเสมอหรือไม่ โดยให้ทำการตรวจสอบอย่างน้อยวันละ ๑ ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบแจ้งผู้ดูแลระบบที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยทันที

๓. นโยบายการห้ามการติดตั้งระบบหรืออุปกรณ์ต่าง ๆ เพิ่มเติม

วัตถุประสงค์

๑. เพื่อป้องกันผลข้างเคียงจากการติดตั้งเครื่องคอมพิวเตอร์ ซอร์ฟแวร์ หรืออุปกรณ์อื่นๆ ที่นอกเหนือจากที่สำนักงานได้ติดตั้งไว้ให้ใช้งาน เช่น เป็นแหล่งที่มาของไวรัส โทรจัน หรือโปรแกรมไม่ประสงค์ดีอื่นๆ หรือใช้เป็นทางเข้าสู่เครือข่ายภายในสำนักงานโดยผู้ไม่ประสงค์ดี

๒. เพื่อป้องกันการเข้าถึงเครือข่าย หรือข้อมูลของสำนักงานโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

ผู้ใช้งาน

อ้างอิงมาตรฐาน

หมวดที่ ๓ การบริหารจัดการทรัพย์สินของสำนักงาน

การดำเนินการ

๑. ห้ามติดตั้งโปรแกรมคอมพิวเตอร์เพิ่มเติมนอกเหนือจากที่สำนักงานได้ติดตั้งไว้ให้ใช้งาน

๒. ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นการติดตั้งเพื่อปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง

๓. ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ หรืออุปกรณ์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครือข่ายของสำนักงาน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์นั้น หรือเครือข่ายของสำนักงานได้

๔. ห้ามนำเครื่องคอมพิวเตอร์ที่ผู้ใช้เป็นเจ้าของมาใช้กับระบบเครือข่ายของสำนักงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบที่เกี่ยวข้องก่อนการใช้งาน

๕. ห้ามเปลี่ยนแปลงเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์แบบตั้งโต๊ะภายในหน่วยงาน

๔. นโยบายการใช้งานอินเตอร์เน็ต

วัตถุประสงค์

เพื่อให้มีการใช้งานอินเตอร์เน็ตที่สำนักงานจัดไว้ให้อย่างเหมาะสมตามภารกิจงานของผู้ใช้งานโดยไม่นำไปใช้ในกิจกรรมอื่นๆ ที่เป็นการสูญเสียเวลาการทำงานโดยไม่มีประโยชน์ ที่มีลักษณะเป็นอบายมุข ที่อาจก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงของสำนักงาน หรือที่ขัดต่อศีลธรรม จริยธรรม ชาติ ศาสนา พระมหากษัตริย์ หรือสิ่งที่บุคคลทั่วไปพึงประพฤติปฏิบัติ

ผู้รับผิดชอบ

ผู้ใช้งาน

อ้างอิงมาตรฐาน

หมวดที่ ๓ การบริหารจัดการทรัพย์สินของสำนักงาน

การดำเนินการ

๑. ห้ามทำการดาวน์โหลด (Download) หรือส่งไฟล์ประเภทสื่อลามกอนาจาร

๒. ห้ามเล่น ดูภาพยนตร์ หรือฟังเพลง ผ่านทางอินเตอร์เน็ตในเวลาทำงาน

๓. ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

๓.๑ การพนัน

๓.๒ การประมูล

๓.๓ การวิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และพระมหากษัตริย์

๓.๔ การลามก อนาจาร

๓.๕ อื่นๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย หรือผิดศีลธรรม จริยธรรม

๔. ห้ามใช้อินเตอร์เน็ตเพื่อส่ง กระจาย หรือแจกจ่าย สื่อหรือข้อมูล ดังต่อไปนี้

๔.๑ สื่อสิ่งพิมพ์อิเล็กทรอนิกส์ที่เป็นการละเมิดลิขสิทธิ์ทางปัญญา

๔.๒ ข้อมูลส่วนบุคคลที่ไม่ได้รับอนุญาตจากผู้เป็นเจ้าของ

๕. ห้ามใช้อินเตอร์เน็ตเพื่อเข้าร่วมกิจกรรมที่อาจก่อให้เกิดความเสียหายต่อภาพลักษณ์และชื่อเสียงของสำนักงาน

๖. หากหน่วยงานมีความประสงค์จะขอใช้เลขที่อยู่ไอพีสาธารณะ (Public IP Address) จะต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บริหารสูงสุดสำนักงาน

๕. นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)

วัตถุประสงค์

เพื่อให้มีการใช้งาน E-Mail ที่สำนักงาน จัดไว้ให้อย่างเหมาะสมตามภารกิจงานของผู้ใช้งาน และไม่ใช้ในกิจกรรมอื่นๆ ที่อาจก่อให้เกิดความเสียหายต่อผู้อื่นหรือต่อสำนักงาน

ผู้รับผิดชอบ

ผู้ใช้งาน

อ้างอิงมาตรฐาน

หมวดที่ ๓ การบริหารจัดการทรัพย์สินของสำนักงาน

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

การดำเนินการ

๑. ห้ามใช้ที่อยู่ E-Mail (E-Mail Address) อื่นๆ นอกเหนือจากที่สำนักงานได้จัดสรรไว้ให้เพื่อใช้ในการติดต่องานตามภารกิจหรือหน้าที่ความรับผิดชอบของตนกับหน่วยงานทั้งภายในและภายนอก

๒. ห้ามผู้ใช้งานเข้าถึงข้อมูล E-Mail ของบุคคลอื่นโดยไม่ได้รับอนุญาต

๓. ห้ามลงทะเบียนด้วยที่อยู่ E-Mail (E-Mail Address) ที่สำนักงานมอบให้ไว้ตามที่อยู่เว็บไซต์ต่างๆ ที่ไม่มีความเกี่ยวข้องกับงานของสำนักงาน

๔. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)]

๕. ห้ามส่ง E-Mail ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

๖. ห้ามส่ง E-Mail ที่มีลักษณะเป็นการละเมิดต่อกฎหมายทรัพย์สินทางปัญญาหรือสิทธิของบุคคลอื่น

๗. ห้ามส่ง E-Mail ที่มีโปรแกรมไม่ประสงค์ดีไปให้กับบุคคลอื่นโดยเจตนา

๘. ห้ามปลอมแปลง E-Mail ของบุคคลอื่น

๙. ห้ามรับหรือส่ง E-Mail แทนบุคคลอื่นโดยไม่ได้รับอนุญาต

๑๐. ห้ามใช้คำที่ไม่สุภาพในการส่ง E-Mail

๑๑. ห้ามส่ง E-Mail ที่มีขนาดใหญ่เกินกว่า ๒๐ เมกกะไบต์ หรือตามขนาดที่สำนักงานระบุไว้

๑๒. ห้ามส่ง E-Mail ที่มีข้อมูลความลับของสำนักงานเว้นเสียแต่ว่าจะใช้วิธีการที่มีความปลอดภัยที่สำนักงานกำหนดไว้

๑๓. ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-Mail ของผู้รับให้ถูกต้อง เพื่อป้องกันการส่งข้อมูลผิดพลาด

๑๔. ให้ระบุชื่อของผู้ส่งใน E-Mail ทุกฉบับที่ส่งไป

๑๕. ให้จำกัดกลุ่มผู้รับ E-Mail เท่าที่มีความจำเป็นต้องรับทราบในข้อมูลที่ส่งไปนั้น

๑๖. ให้ทำการสำรองข้อมูล E-Mail ตามความจำเป็นอย่างสม่ำเสมอ

๖. นโยบายการป้องกันการใช้ระบบเครือข่ายผิดวัตถุประสงค์

วัตถุประสงค์

เพื่อป้องกันการใช้ระบบเครือข่ายผิดวัตถุประสงค์

ผู้รับผิดชอบ

ผู้ใช้งาน

อ้างอิงมาตรฐาน

หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

การดำเนินการ

ผู้ใช้งานจะต้องไม่ใช้ระบบเครือข่ายของสำนักงานโดยมีวัตถุประสงค์ ดังต่อไปนี้

๑. เพื่อกระทำการผิดกฎหมายหรือเพื่อก่อให้เกิดความเสียหายแก่บุคคลอื่น

๒. เพื่อกระทำการที่ขัดต่อ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๓. เพื่อกระทำการที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๔. เพื่อค้าขายส่วนตัว

๕. เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของสำนักงานหรือของบุคคลอื่น

๗. เพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

๘. เพื่อรับหรือส่งข้อมูลซึ่งอาจก่อให้เกิดความเสียหายต่อสำนักงาน เช่น การส่งข้อมูลที่มีลักษณะเป็นจดหมายลูกโซ่ การส่งข้อมูลอันมีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น เป็นต้น

๙. เพื่อขัดขวางหรือทำให้ไม่สามารถใช้งานได้ตามปกติ การใช้งานเครือข่ายคอมพิวเตอร์ของสำนักงานของเจ้าหน้าที่อื่น หรือของหน่วยงานภายนอกอื่น

๑๐. เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของสำนักงาน ไปยังที่อยู่เว็บไซต์ใด ๆ ในลักษณะที่จะก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

๑๑. เพื่อกระทำการอื่นใดที่อาจขัดต่อผลประโยชน์ของสำนักงานหรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายต่อสำนักงาน

๗. นโยบายการป้องกันข้อมูลพิสูจน์ตัวตนในการเข้าใช้งานระบบ (Username) และรหัสผ่าน (Password)

วัตถุประสงค์

เพื่อป้องกันการถึงข้อมูล ระบบ อุปกรณ์ หรือทรัพยากรสารสนเทศอื่น ๆ ของสำนักงาน โดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

ผู้ใช้งาน

อ้างอิงมาตรฐาน

หมวดที่ ๗ การควบคุมการเข้าถึง

การดำเนินการ

๑. เมื่อผู้เข้าใช้งานระบบ ควรจะมีการเปลี่ยนรหัสผ่านทุกๆ ๓ เดือน โดยตั้งรหัสผ่านตามแนวทางปฏิบัติดังนี้

๑.๑ มีการผสมผสานกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกันอย่างน้อย ๖ ตัว

๑.๒ ไม่กำหนดรหัสผ่านจากชื่อ หรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน

๑.๓ ไม่กำหนดรหัสผ่านจากคำศัพท์ที่ปรากฏในพจนานุกรม

๒. เก็บรักษารหัสผ่านของตนเองไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น

๓. กำหนดรหัสผ่านให้มีคุณสมบัติ ตามนโยบายการตั้งรหัสผ่าน

๔. กำหนดรหัสผ่านสำหรับการใช้ไฟล์ข้อมูลร่วมกันกับบุคคลอื่นโดยผ่านทางระบบเครือข่าย

๕. ห้ามบันทึกรหัสผ่านไว้ในโปรแกรมคอมพิวเตอร์เพื่อช่วยในการจำรหัสผ่านของตน

๖. ต้องไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น

๗. ในกรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเพื่อให้สามารถปฏิบัติงานแทนตนเองได้หลังจากที่ทำงานนั้นเสร็จเรียบร้อยแล้วให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๘. นโยบายการเข้าไปปฏิบัติงานในห้องคอมพิวเตอร์แม่ข่ายกลาง (Server Room)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงทางกายภาพโดยอนุญาตให้เฉพาะผู้ที่มีภารกิจเท่านั้น จึงจะสามารถเข้าถึงห้องคอมพิวเตอร์แม่ข่ายกลางได้ และป้องกันการสูญหาย เสียหาย การถูกขโมยของทรัพย์สินต่าง ๆ ในห้องคอมพิวเตอร์แม่ข่ายกลาง รวมทั้งการเข้าถึงระบบโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

ผู้ใช้งาน

อ้างอิงมาตรฐาน

หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

การดำเนินการ

๑. ห้ามเข้าไปในบริเวณห้องคอมพิวเตอร์แม่ข่ายกลางโดยไม่มีภารกิจที่เกี่ยวข้องหรือจำเป็น

๒. ห้ามใส่รองเท้าเข้าไปในห้องคอมพิวเตอร์แม่ข่ายกลาง

๓. ห้ามนำอาหาร และเครื่องดื่มเข้าไปในบริเวณห้องคอมพิวเตอร์แม่ข่ายกลาง

๔. ลงบันทึกการเข้าห้องเครื่องในสมุดบันทึกการเข้า-ออกห้องคอมพิวเตอร์แม่ข่ายกลาง

๕. หากพบเห็นความผิดปกติภายในห้องเครื่องคอมพิวเตอร์แม่ข่ายกลาง เช่น มีทรัพย์สินหาย มีร่องรอยการบุกรุก เป็นต้น ให้รีบแจ้งผู้ดูแลระบบที่เกี่ยวข้อง

๖. ปฏิบัติตามคำแนะนำของเจ้าหน้าที่ที่ดูแลห้องคอมพิวเตอร์แม่ข่ายกลางอย่างเคร่งครัด

๙. นโยบายการจัดการเอกสารลับบนกระดาษ หรือบนสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

วัตถุประสงค์

๑. เพื่อป้องกันการเข้าถึงข้อมูลบนสื่อบันทึกข้อมูลโดยไม่ได้รับอนุญาต รวมทั้งป้องกันการรั่วไหลของข้อมูล

๒. เพื่อให้มีวิธีปฏิบัติที่ปลอดภัยในการทำลายข้อมูลบนสื่อบันทึกข้อมูล

ผู้รับผิดชอบ

ผู้ใช้งาน

อ้างอิงมาตรฐาน

หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

การดำเนินการ

๑. ป้องกันเอกสารลับที่ถูกพิมพ์ออกมาทางเครื่องพิมพ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒. จัดหมวดหมู่เอกสารลับไว้ต่างหาก จัดเก็บแยกต่างหาก และต้องป้องกันให้มีความปลอดภัยอย่างพอเพียง

๓. จำกัดการสำเนาเอกสารลับเท่าที่จำเป็นต้องใช้งานเท่านั้น

๔. ระมัดระวังการกระจาย ส่ง หรือแจกจ่ายเอกสารลับไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับทราบ หรือใช้งานเอกสารนั้นเท่านั้น

๕. ใช้วิธีการตามกฎหมายที่หน่วยงานได้ถือปฏิบัติอยู่แล้วสำหรับการจัดส่งเอกสารลับทางไปรษณีย์

๖. เมื่อมีความจำเป็นต้องทำลายข้อมูลลับบนสื่อบันทึกข้อมูล ให้ปฏิบัติตามขั้นตอนปฏิบัติสำหรับการทำลายข้อมูลบนสื่อบันทึกข้อมูล (Procedure for Media Disposal) ดังนี้

๖.๑ คัดแยกเอกสารบนสื่อบันทึกข้อมูลทั้งที่แน่ใจว่าเป็นเอกสารลับและไม่แน่ใจว่าลับหรือไม่ ให้อยู่ในกลุ่มเอกสารลับ

๖.๒ ทำลายเอกสารลับเหล่านั้นโดยใช้วิธีการดังนี้

- สำหรับเอกสารลับบนกระดาษ ห้ามนำกลับมาใช้อีกครั้งแม้ว่ายังสามารถใช้งานได้อีกด้านหนึ่งให้ทำลายด้วยเครื่องหั่นทำลายเอกสารและ/หรือซีดี
- สำหรับเอกสารลับบนฮาร์ดดิสก์ (Hard Disk) ให้ใช้วิธีการฟอร์แม๊ต (Format)
- สำหรับเอกสารลับบนซีดีหรือดีวีดี ให้ทำลายด้วยเครื่องหั่นทำลายเอกสารและ/หรือซีดี

๑๐. นโยบายการลงทะเบียนการใช้งานระบบสารสนเทศ/ระบบเครือข่ายคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงระบบโดยอนุญาตให้เข้าถึงได้ตามความจำเป็นในการใช้งาน

๒. เพื่อป้องกันผู้ใช้ปฏิเสธการใช้งานโดยจัดให้มีการลงทะเบียนและจัดทำบัญชีผู้ใช้แยกเป็นผู้ใช้รายบุคคลและผู้ใช้ร่วมกัน

ผู้รับผิดชอบ

ผู้ใช้งาน

อ้างอิงมาตรฐาน

หมวดที่ ๗ การควบคุมการเข้าถึง

การดำเนินการ

๑. ห้ามผู้ให้ใช้ระบบงานของสำนักงานจนกว่าจะได้รับการอนุมัติให้ใช้งานโดยผ่านการลงทะเบียนก่อน รวมทั้งต้องไม่พยายามเข้าถึงระบบงานใด ๆ ก็ตามที่ตนยังไม่ได้รับอนุมัติให้ใช้งาน

๒. กรอกแบบคำขอเพื่อขออนุมัติใช้งานระบบงานตาม**แบบฟอร์มคำขอใช้บริการระบบ(เครือข่ายคอมพิวเตอร์/ระบบสารสนเทศ)** และนำเสนอต่อผู้บังคับบัญชาเพื่อขออนุมัติใช้งาน เมื่อได้รับการอนุมัติแล้วให้ส่งผู้บังคับบัญชาของผู้ดูแลระบบและ/หรือผู้พัฒนาระบบเพื่อดำเนินการต่อไป

๓. ในกรณีที่มีความจำเป็นต้องมีการใช้งานบัญชีผู้ใช้ร่วมกัน ให้ขออนุมัติผู้บังคับบัญชาระดับกลุ่ม/ฝ่ายตามแบบฟอร์มฯหากมีความเสียหายเกิดขึ้น ผู้ที่ใช้งานบัญชีร่วมกันนั้นจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นร่วมกัน เมื่อได้รับการอนุมัติแล้วให้ส่งต่อผู้บังคับบัญชาของผู้ดูแลระบบและ/หรือผู้พัฒนาระบบเพื่อดำเนินการต่อไป

๑๑. นโยบายการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัย

วัตถุประสงค์

เพื่อให้มีการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย เพื่อนำผลที่ได้ไปสู่การบริหารจัดการรวมทั้งดำเนินการแก้ไขได้อย่างเหมาะสม ได้ผล และทันกาล

ผู้รับผิดชอบ

ผู้ใช้งาน

อ้างอิงมาตรฐาน

หมวดที่ ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสำนักงาน

การดำเนินการ

๑. แจ้งไปยังผู้ดูแลระบบที่เกี่ยวข้อง (กลุ่มระบบคอมพิวเตอร์และเครือข่าย/กลุ่มระบบสารสนเทศและภูมิสารสนเทศ) โดยทันที เมื่อพบเห็น

๑.๑ การกระทำที่ขัดต่อ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๑.๒ การกระทำที่ขัดต่อความมั่นคงของชาติ

๑.๓ การใช้ทรัพยากรสารสนเทศของสำนักงานผิดวัตถุประสงค์

๑.๔ หน้าเว็บไซต์หลักถูกเปลี่ยนแปลง

๑.๕ ข้อมูลในหน้าเว็บไซต์หลักไม่ถูกต้อง หรือคลาดเคลื่อนจากความเป็นจริง

๑.๖ ข้อมูลสำคัญถูกเปลี่ยนแปลง ถูกลบ หรือสูญหาย

๑.๗ การเปิดเผยข้อมูลสำคัญ หรือข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต

๑.๘ การนำข้อมูลสำคัญไปใช้ผิดวัตถุประสงค์

๑.๙ ทรัพยากรสารสนเทศถูกขโมย

๑.๑๐ การอนุญาตให้บุคคลภายนอกเข้าใช้ระบบของสำนักงาน

๑.๑๑ การแอบติดตั้งอุปกรณ์ หรือโปรแกรมเพื่อดักขโมยข้อมูล หรือดักดูข้อมูลในเครือข่าย

๑.๑๒ การใช้อำนาจของสิทธิการเป็นผู้ดูแลระบบอย่างไม่เหมาะสม

๑.๑๓ การบุกรุกห้องคอมพิวเตอร์แม่ข่ายกลาง

๑.๑๔ โปรแกรมไม่ประสงค์ดี

๑.๑๕ เหตุการณ์อื่น ๆ ที่เป็นการละเมิดนโยบายด้านความมั่นคงปลอดภัยของสำนักงาน

๒. ให้ความร่วมมือและอำนวยความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลระบบที่เกี่ยวข้องในการตรวจสอบเหตุการณ์ทางด้านความมั่นคงปลอดภัยที่เกิดขึ้น รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชา และผู้ดูแลระบบที่เกี่ยวข้องด้วย

ส่วนที่ ๓
นโยบายการจัดการระบบคอมพิวเตอร์และเครือข่าย
สำหรับเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ

นโยบายการจัดการระบบคอมพิวเตอร์และเครือข่าย ประกอบด้วย

๑. นโยบายการจัดทำคู่มือการปฏิบัติงาน

วัตถุประสงค์

เพื่อให้การปฏิบัติงานด้านสารสนเทศเป็นไปอย่างถูกต้อง ลดความผิดพลาดที่อาจเกิดขึ้นซึ่งอาจส่งผลให้เกิดการหยุดชะงักการทำงาน

ผู้รับผิดชอบ

ผู้ดูแลระบบและผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

การดำเนินการ

ให้จัดทำและปรับปรุงคู่มือการปฏิบัติงานให้มีความทันสมัย อย่างน้อยให้ครอบคลุมในรายการคู่มือการปฏิบัติงานของสำนักงาน รวมทั้งให้จัดเก็บไว้ในสถานที่ที่มีความปลอดภัย

๒. นโยบายการพัฒนาระบบงาน

วัตถุประสงค์

๑. เพื่อลดความผิดพลาดในการพิจารณาปรับปรุงระบบงานเพิ่มเติม

๒. เพื่อให้ระบบงานได้รับการพัฒนาเพื่อให้ประมวลผลหรือคำนวณได้อย่างถูกต้องและเพื่อให้ข้อมูลนำเข้าและนำออกจากระบบมีความถูกต้องและเชื่อถือได้ รวมทั้งปลอดภัยจากการถูกบุกรุกหรือเจาะระบบโดยผู้ไม่ประสงค์ดี

๓. เพื่อให้ระบบงานที่พัฒนาหรือจัดหาเป็นไปตามข้อกำหนดหรือคุณลักษณะของระบบที่กำหนดไว้

๔. เพื่อให้สามารถตรวจสอบกิจกรรมสำคัญต่าง ๆ ที่เกิดกับระบบงานได้ในภายหลัง

๕. เพื่อลดความผิดพลาดในการติดตั้งระบบงานและอาจส่งผลให้ระบบหยุดชะงักการทำงาน

ผู้รับผิดชอบ

ผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับสำนักงาน

หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

การดำเนินการ

๑. จัดให้มีการกรอกแบบคำขอเพื่อขออนุมัติพัฒนาระบบงานใหม่หรือปรับปรุงระบบงานเดิม และปฏิบัติตาม**ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบงาน** ที่ได้กำหนดไว้

๒. กำหนดการควบคุมระบบงาน (Application Control) ดังนี้

๒.๑ ออกแบบระบบเพื่อให้สามารถตรวจสอบความถูกต้องของข้อมูลนำเข้า โดยปฏิบัติตาม**แนวทางปฏิบัติในการตรวจสอบข้อมูลนำเข้า**

๒.๒ ออกแบบระบบเพื่อให้สามารถตรวจสอบความถูกต้องของการประมวลผลข้อมูลที่เกิดขึ้นโดยปฏิบัติตาม**แนวทางปฏิบัติในการตรวจสอบความถูกต้องของการประมวลผลข้อมูล**

๓. ตรวจสอบความถูกต้องของรายงานต่าง ๆ ในระหว่างที่ทำการพัฒนาและหากพบข้อผิดพลาดให้ตรวจสอบหาสาเหตุ และดำเนินการแก้ไข

๔. พัฒนาระบบงานตาม**มาตรฐานทางด้านความมั่นคงปลอดภัยในการพัฒนาระบบงาน**

๕. จัดทำเอกสารข้อกำหนด (TOR) โดยระบุคุณลักษณะของระบบที่ต้องการจัดหาไว้ในเอกสารดังกล่าว

๖. จัดทำสัญญาสำหรับการจัดซื้อจัดจ้างระบบงานโดย

๖.๑ อ้างอิงตามข้อกำหนดต่าง ๆ ที่ระบุไว้ใน

- ข้อกำหนดที่ควรจัดทำในสัญญาการพัฒนาระบบงาน
- ข้อกำหนดที่ควรจัดทำในสัญญาการบำรุงรักษาห้องคอมพิวเตอร์แม่ข่ายกลาง

- ข้อกำหนดที่ควรจัดทำในสัญญาดูแลรักษาฮาร์ดแวร์
- ข้อกำหนดที่ควรจัดทำในสัญญาการให้บริการเครือข่าย
- ข้อกำหนดที่ควรจัดทำในสัญญาการให้บริการความช่วยเหลือ

๖.๒ ข้อกำหนดการไม่เปิดเผยข้อมูลของงานที่ดำเนินการตามสัญญาแก่บุคคลอื่นใด

๗. ให้พัฒนาระบบงานเพื่อบันทึกล็อก (Log) ตามประเภทของข้อมูลดังนี้

๗.๑ ข้อมูลที่เกี่ยวข้องกับการพิสูจน์ตัวตนในการเข้าใช้งานระบบงาน เช่น username และวันเวลาที่เข้าใช้งาน เป็นต้น

๗.๒ ข้อมูลประเภทข้อผิดพลาด (Error Log) ที่จำเป็นต้องตรวจสอบในภายหลัง เช่น การคำนวณผิดพลาด การเชื่อมต่อเข้าระบบบริหารจัดการฐานข้อมูลที่ไม่สำเร็จ เป็นต้น

๗.๓ ข้อมูลที่ใช้สำหรับการผูกพันหน้าที่ความรับผิดชอบของผู้ทำธุรกรรม เช่น ข้อมูลว่าใครเป็นผู้บันทึกข้อมูลเข้าระบบ

๗.๔ ข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตามที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และประกาศข้อกำหนดการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้กำหนดไว้

๗.๕ ข้อมูลที่มีความสำคัญอื่น ๆ ซึ่งจำเป็นต้องตรวจสอบในภายหลัง

๘. ให้ทำการทดสอบระบบงาน และบันทึกผลการทดสอบไว้ด้วยตาม

๘.๑ ข้อกำหนดทางด้านความมั่นคงปลอดภัย

๘.๒ แนวทางปฏิบัติการตรวจสอบข้อมูลนำเข้า

๙. ปฏิบัติตามนโยบายควบคุมการติดตั้งบนระบบให้บริการจริงในการติดตั้งระบบงาน

๓. นโยบายควบคุมการติดตั้งบนระบบให้บริการจริง

วัตถุประสงค์

๑. เพื่อลดความผิดพลาดในการติดตั้งระบบงานและอาจส่งผลให้ระบบหยุดชะงักการทำงานหรือไม่สามารถให้บริการได้

๒. เพื่อให้ระบบที่ติดตั้งมีความมั่นคงปลอดภัยและเสถียรภาพในการทำงานสูง

๓. เพื่อป้องกันการละเมิดลิขสิทธิ์ของซอฟต์แวร์ที่จะทำการติดตั้ง

๔. เพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขระบบงานโดยไม่ได้รับอนุญาต และทำให้ระบบงานทำงานไม่ถูกต้องและอาจเกิดความเสียหายต่อสำนักงาน

ผู้รับผิดชอบ

ผู้ดูแลระบบ และ/หรือ ผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

การดำเนินการ

๑. ปฏิบัติตามขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศเพื่อขออนุมัติติดตั้งระบบงาน

๒. สำหรับการเปลี่ยนแปลงที่มีผลกระทบมากให้จัดเตรียมแผนถอยหลังกลับก่อนดำเนินการเปลี่ยนแปลงใด ๆ ซึ่งอย่างน้อยจะต้องประกอบด้วยการสำรองข้อมูลในฐานข้อมูล และซอฟต์แวร์ (Software) ต่าง ๆ ที่เกี่ยวข้องกับระบบงานนั้น

๓. กำหนดแผนการติดตั้งสำหรับระบบงาน (ซึ่งรวมถึงระยะเวลาที่จะดำเนินการ) รวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า

๔. สำหรับซอฟแวร์ (Software) ที่จะทำการติดตั้ง

๔.๑ ถ้าเป็นซอฟต์แวร์ (Software) ที่ขายเชิงพาณิชย์ต้องเป็นซอฟแวร์ (Software) ที่มีลิขสิทธิ์ถูกต้อง

๔.๒ ถ้าเป็นซอฟต์แวร์ (Software) ประเภทฟรีแวร์ (Freeware) หรือแชร์แวร์ (Shareware) ต้องตรวจสอบก่อนว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตนั้น

๕. สำหรับการติดตั้งซอฟต์แวร์ยูลิตี้ (Software Utility) ต้องได้รับการอนุมัติจากผู้บังคับบัญชาของผู้พัฒนาระบบ/ผู้ดูแลระบบก่อน จึงจะสามารถติดตั้งได้

๖. รวบรวมและจัดเก็บซอร์สโค้ด (Source Code) ของระบบงานทั้งหมดไว้ในสถานที่เดียวกันที่มีความปลอดภัย และควบคุมให้มีเวอร์ชัน (Version) ของซอร์สโค้ด (Source Code) อย่างน้อย ๒ เวอร์ชั่น (Version) ล่าสุด และกำหนดให้ผู้ที่เกี่ยวข้องเท่านั้นที่สามารถเข้าถึงได้

๔. นโยบายการลงทะเบียนผู้ใช้

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงระบบโดยอนุญาตให้เข้าถึงได้ตามความจำเป็นในการใช้งาน

๒. เพื่อกำหนดมาตรฐานการลงทะเบียนผู้ใช้และการบริหารจัดการบัญชีผู้ใช้

๓. เพื่อกำหนดและทบทวนสิทธิการใช้งานเพื่อให้ได้รับสิทธิตามความจำเป็นในการใช้งาน

ผู้รับผิดชอบ

ผู้ดูแลระบบ และ/หรือ ผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๗ การควบคุมการเข้าถึง

การดำเนินการ

๑. จัดให้มีการลงทะเบียนผู้ใช้ก่อนอนุญาตให้เข้าใช้ระบบงานต่าง ๆ ของสำนักงาน โดยให้ขออนุมัติผ่านทาง **แบบคำขอสำหรับลงทะเบียนผู้ใช้ระบบงาน**

๒. ตั้งชื่อบัญชีผู้ใช้ตามแนวทางการกำหนดข้อมูลพิสูจน์ตัวตนในการเข้าใช้ระบบ (Username) ดังนี้

๒.๑ ใช้ชื่อภาษาอังกฤษตามที่ใช้ในบัญชี E-mail ที่สำนักงานกำหนดให้ เช่น somchai_tr@opsmoac.go.th หรือ somchai_tr เป็นต้น

๒.๒ ใช้ชื่อภาษาอังกฤษตามบัตรประจำตัวประชาชนหรือหนังสือเดินทางถูกต้องตามระบบฐานข้อมูลการบริหารทรัพยากรบุคคลของสำนักงานปลัดกระทรวงเกษตรและสหกรณ์ (DPIS)

๒.๓ กำหนดรหัสผ่านให้มีความยาวไม่น้อยกว่า ๖ ตัวอักษร

๓. จัดส่งบัญชีผู้ใช้และรหัสผ่านโดยใส่ซองปิดผนึกและประทับตรา “ลับ” และแนบเอกสารนโยบายความมั่นคงปลอดภัยในส่วนของผู้ใช้งานไปด้วย

๔. สร้างบัญชีผู้ใช้แยกเป็นรายบุคคล ในกรณีที่มีความจำเป็นต้องใช้งานบัญชีผู้ใช้ร่วมกันให้ขออนุมัติเป็นกรณีไป

๕. กำหนดสิทธิการเข้าใช้งานระบบงานให้แก่ผู้ใช้ตามหน้าที่และความรับผิดชอบของผู้ใช้นั้นหรือตามความจำเป็นในการเข้าถึง (ทั้งเจ้าหน้าที่และบุคคลภายนอกที่สำนักงานอนุญาตให้ใช้งาน)

๖. ทบทวนสิทธิการเข้าใช้งานระบบของผู้ใช้อย่างน้อยปีละ ๑ ครั้ง

๕. นโยบายการบริหารจัดการช่องโหว่ของระบบ

วัตถุประสงค์

เพื่อให้ระบบทำงานอย่างถูกต้อง มีเสถียรภาพ เชื่อถือได้ และปลอดภัยจากการถูกบุกรุกหรือโจมตี

ผู้รับผิดชอบ

ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

การดำเนินการ

๑. ติดตั้ง Patch ตามความจำเป็นสำหรับช่องโหว่ที่มีผลกระทบต่อการให้บริการของเครื่องแม่ข่ายสำหรับระบบงานของสำนักงาน

๒. จัดให้เครื่องคอมพิวเตอร์ (Personal Computer) และโน้ตบุกส์ (Notebook Computer) ทั้งหมดของผู้ใช้ติดตั้ง Patch ให้ครบ (เช่น โดยการตั้งให้เครื่องดำเนินการเองโดยอัตโนมัติ)

๖. นโยบายการจัดการกับโปรแกรมไม่ประสงค์ดี

วัตถุประสงค์

๑. เพื่อป้องกันข้อมูลในระบบไม่ให้เกิดความเสียหาย

๒. เพื่อให้มีการจัดการกับปัญหาไวรัสได้อย่างเหมาะสม ได้ผล และทันกาล

๓. เพื่อให้ระบบทำงานอย่างถูกต้อง มีเสถียรภาพ เชื่อถือได้ และปลอดภัยจากถูกบุกรุกหรือโจมตี

ผู้รับผิดชอบ

ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

การดำเนินการ

๑. จัดให้ผู้ใช้แจ้งปัญหาการติดไวรัสไปยังผู้ดูแลระบบโดยทันทีที่พบ

๒. บันทึกปัญหาการติดไวรัส และวิธีการแก้ไข

๓. ตรวจสอบว่าเครื่องแม่ข่ายป้องกันไวรัสยังทำงานตามปกติ และมีการปรับปรุงฐานข้อมูลไวรัส (Virus signature) หรือไม่ตรวจสอบอย่างน้อยวันละ ๑ ครั้ง หากพบว่าทำงานผิดปกติให้รีบดำเนินการแก้ไข

๔. ตรวจสอบและติดตั้งโปรแกรมป้องกันไวรัสอย่างน้อยสำหรับเครื่องลูกข่ายทั้งหมด เครื่องแม่ข่ายสำหรับระบบงานที่มีความสำคัญ

๕. ตรวจสอบและติดตั้งโปรแกรมป้องกันไวรัสให้กับผู้ใช้งานเพื่อให้ทำงานในลักษณะทันทีทันใด (Real Time Scan) เมื่อมีการเปิดไฟล์ขึ้นมาใช้งานโปรแกรมป้องกันไวรัสจะทำการสแกน (Scan) ทันที

๗. นโยบายการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย

วัตถุประสงค์

๑. เพื่อให้มีการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยและบริหารจัดการรวมทั้งดำเนินการแก้ไขได้อย่างเหมาะสม ได้ผล และทันกาล

๒. เพื่อนำผลที่ได้ไปปรับปรุงการบริหารจัดการความมั่นคงปลอดภัยให้ดียิ่งขึ้น

ผู้รับผิดชอบ

ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

หมวดที่ ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสำนักงาน

การดำเนินการ

๑. เมื่อได้รับรายงานเหตุการณ์เกี่ยวกับโปรแกรมไม่ประสงค์ดีจากผู้ใช้ ให้ปฏิบัติตามขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี เพื่อดำเนินการแก้ไขเหตุการณ์ดังกล่าว

๒. เมื่อได้รับรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยอื่น ๆ ให้ปฏิบัติตามขั้นตอนปฏิบัติสำหรับการจัดการกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยเพื่อดำเนินการแก้ไขเหตุการณ์ดังกล่าว

๘. นโยบายการจัดการความมั่นคงปลอดภัยสำหรับระบบสารสนเทศและเครือข่าย

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศและเครือข่ายมีความมั่นคงปลอดภัย มีเสถียรภาพและความเชื่อถือได้สูง และมีความมั่นคงปลอดภัยจากการถูกเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต

๒. เพื่อควบคุมการเข้าถึงระบบบนเครือข่ายให้เป็นไปตามนโยบายควบคุมการเข้าถึง

๓. เพื่อลดความผิดพลาดในการเปลี่ยนแปลงระบบซึ่งอาจส่งผลให้ระบบหยุดชะงักการทำงานหรือไม่สามารถให้บริการได้

๔. เพื่อให้มีการปฏิบัติที่สอดคล้องกับกฎหมาย พ.ร.บ. หรือข้อบังคับภายนอกอื่นๆ ที่ได้กำหนดไว้

ผู้รับผิดชอบ

ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

หมวดที่ ๗ การควบคุมการเข้าถึง

หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

การดำเนินการ

๑. จัดทำและปรับปรุงเครื่องแม่ข่ายพร็อกซี่ (Proxy) เพื่อช่วยลดปริมาณข้อมูลในเครือข่าย

๒. จำกัดการเข้าถึงระบบและอุปกรณ์เครือข่ายสำคัญเพื่อให้การเข้าถึงนั้นจะต้องมาจากอุปกรณ์ ระบบ หรือสถานที่ที่ได้รับอนุญาตแล้วเท่านั้น

๓. ตรวจสอบและปิดพอร์ต (Port) ของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ

๔. ปรับปรุงผังเครือข่ายให้มีความทันสมัยอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

๕. ให้ใช้**โปรแกรมมาตรฐานที่มีการเข้ารหัสข้อมูลสำหรับการเชื่อมต่อจากภายใน**เครือข่ายเพื่อเข้าสู่เครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายต่างๆ (สำนักงานต้องกำหนดโปรแกรมนี้ขึ้นมาและใช้เป็นมาตรฐานเดียวกันในการเชื่อมต่อไปยังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่าย)

๖. ให้ใช้**โปรแกรมมาตรฐานที่มีการเข้าถึงข้อมูลสำหรับการเชื่อมต่อจากระยะไกล**ภายนอกสำนักงานเข้ามาสู่เครือข่ายภายในสำนักงาน (สำนักงานต้องกำหนดโปรแกรมขึ้นมา และใช้เป็นมาตรฐานเดียวกันในการเชื่อมต่อจากภายนอกเข้ามา)

๗. จัดทำและปรับปรุงระบบสำหรับการพิสูจน์ตัวตนก่อนเข้าใช้ระบบสำคัญต่างๆ เพื่อให้มีความมั่นคงปลอดภัยมากขึ้น

๘. ตรวจสอบและจัดแบ่งเครือข่ายของสำนักงานให้มีความมั่นคงปลอดภัยโดยใช้แนวทางการแบ่งเครือข่ายดังนี้

๘.๑ การแยกตาม กอง/สำนัก/หน่วยงานหรือที่ตั้งอาคารของสำนักงาน

๘.๒ การแยกตามลักษณะงานของสำนักงาน (เช่น จัดให้เครื่องลูกข่ายที่มีลักษณะงานคล้ายกันอยู่ในวงเครือข่ายเดียวกัน)

๙. ตรวจสอบและจำกัดการเชื่อมต่อทางเครือข่ายให้เหมาะสมโดยผ่านทางอุปกรณ์เครือข่ายเพื่อให้เป็นไปตาม**นโยบายควบคุมการเข้าถึง**ของสำนักงาน

๑๐. ตรวจสอบและกำหนดเส้นทางบนเครือข่ายให้เหมาะสมโดยผ่านทางอุปกรณ์เครือข่าย เพื่อควบคุมการเชื่อมต่อทางเครือข่ายให้เป็นไปตาม**นโยบายควบคุมการเข้าถึง**

๑๑. เฝ้าระวัง ติดตาม และตรวจสอบการทำงานของระบบหรืออุปกรณ์ต่างๆ อย่างสม่ำเสมอเพื่อป้องกันกิจกรรมที่ไม่ได้รับอนุญาตหรือการเข้าถึงโดยไม่ได้รับอนุญาต

๑๒. ตรวจสอบและติดตั้งสัญญาณนาฬิกาของระบบหรืออุปกรณ์ต่างๆ ให้ถูกต้องตามเวลามาตรฐานสากล

๑๓. กรอกแบบคำขอเพื่อขออนุมัติดำเนินการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนทศต่างๆ และปฏิบัติตาม**ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ**ที่กำหนดไว้

๑๔. ห้ามเปิดช่องทางการเชื่อมต่อทางเครือข่ายจากภายนอกเข้าสู่เครือข่ายภายในสำนักงาน เพื่อให้สามารถเข้าถึงเครื่องแม่ข่ายสำหรับระบบงานได้จากระยะไกล ยกเว้นในกรณีที่มีความจำเป็นหรือมีความเร่งด่วนสูง ซึ่งจะต้องได้รับอนุมัติจากผู้บังคับบัญชาก่อนดำเนินการ และกำหนดให้ใช้ในระยะเวลา ๗ วัน รวมทั้งต้องใช้วิธีการที่มีความปลอดภัยที่เป็นมาตรฐานสำหรับการเชื่อมต่อจากระยะไกลที่สำนักงานกำหนดไว้ หลังจากที่สิ้นสุดการใช้งาน ให้ทำการปิดช่องทางการเชื่อมต่อนั้นโดยทันที

๙. นโยบายการจัดการทรัพยากรของระบบ

วัตถุประสงค์

เพื่อให้ระบบงานหรืออุปกรณ์มีเสถียรภาพและความเชื่อถือได้สูง

ผู้รับผิดชอบ

ผู้ดูแลระบบ และ/หรือผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

การดำเนินการ

๑. จัดทำระเบียนข้อมูลบัญชีทรัพย์สินสารสนเทศ ประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร ข้อมูลและบริการ

๒. ติดตามและตรวจสอบระดับประสิทธิภาพและขีดความสามารถของระบบงานหรืออุปกรณ์สำคัญอย่างสม่ำเสมอ โดยดูจากข้อมูลปริมาณการใช้งานซีพียู (CPU) หน่วยความจำ ฮาร์ดดิสก์ (Hard Disk) และเครือข่าย เพื่อดูว่ายังมีทรัพยากรเพียงพอต่อการให้บริการหรือไม่ รวมทั้งบันทึกไว้เป็นข้อมูลสถิติด้วย

๓. ประเมินประสิทธิภาพและขีดความสามารถของระบบงานหรืออุปกรณ์สำคัญที่ต้องการเพิ่มเติมเพื่อนำไปใช้ในการวางแผนเพื่อปรับปรุงประสิทธิภาพและขีดความสามารถของระบบต่อไป

๔. รายงานข้อมูลสถิติปริมาณการใช้ซีพียู (CPU) หน่วยความจำ ฮาร์ดดิสก์ (Hard Disk) และเครือข่ายของระบบหรืออุปกรณ์สำคัญให้ผู้บังคับบัญชาได้รับทราบอย่างสม่ำเสมอ

๕. สำหรับระบบงานหรืออุปกรณ์สำคัญ ให้พิจารณาจัดหาระบบหรืออุปกรณ์ที่มีความทนทานต่อความผิดพลาด หรือมีองค์ประกอบภายในระบบที่สามารถทำงานทดแทนซึ่งกันและกันได้เมื่อองค์ประกอบหนึ่งเกิดความล้มเหลวหรือเสียหาย

๑๐. นโยบายการแลกเปลี่ยนสารสนเทศระหว่างสำนักงาน

วัตถุประสงค์

เพื่อให้ข้อมูลที่แลกเปลี่ยนกันมีความมั่นคงปลอดภัย ถูกต้อง เชื่อถือได้ รวมทั้งป้องกันความเสียหายและการเข้าถึงโดยไม่ได้รับอนุญาต

ผู้รับผิดชอบ

ผู้บังคับบัญชาผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

การดำเนินการ

๑. จัดทำมาตรการป้องกันข้อมูลสำคัญที่มีการแลกเปลี่ยนกันระหว่างสำนักงานอย่างเป็นทางการโดยกล่าวถึงประเด็นสำคัญดังนี้

๑.๑. ขอบเขตของการป้องกัน

๑.๒ วัตถุประสงค์ในการป้องกัน

๑.๓ ความจำเป็นในการป้องกันข้อมูล

๑.๔ ชนิดของข้อมูลที่แลกเปลี่ยนกันและชั้นความลับ เป็นต้น

๑๑. นโยบายการสำรองและการกู้คืนข้อมูล

วัตถุประสงค์

๑. เพื่อให้มีข้อมูลสำรองไว้ใช้สำหรับระบบต่าง ๆ ในกรณีที่ข้อมูลหลักเกิดความเสียหายหรือไม่สามารถใช้งานหรือเข้าถึงได้

๒. เพื่อให้มั่นใจได้ว่าข้อมูลที่สำรองไว้สำหรับระบบเหล่านั้นสามารถใช้งานได้จริง

๓. เพื่อให้มีการบริหารจัดการเพื่อสร้างความต่อเนื่องให้กับกระบวนการของสำนักงานเมื่อมีเหตุการณ์ที่ทำให้เกิดการหยุดชะงักหรือติดขัดต่อกระบวนการดังกล่าว

ผู้รับผิดชอบ

ผู้บังคับบัญชาของผู้ดูแลระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

หมวดที่ ๑๐ การบริหารความต่อเนื่องในการดำเนินงานของสำนักงาน

หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

การดำเนินการ

๑. กำหนดระบบที่มีความสำคัญทั้งหมดของสำนักงาน และจัดทำเป็นบัญชีรายชื่อของระบบดังกล่าวรวมทั้งปรับปรุงรายชื่อระบบสำคัญและบัญชีฯ ตามความเป็นจริง

๒. กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๓. กำหนดชนิดของข้อมูลของระบบเหล่านั้นที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้อย่างน้อยต้องประกอบด้วย

๓.๑ ข้อมูลค่าคอนฟิกกูเรชัน (Configuration) สำหรับระบบ

๓.๒ ข้อมูลคู่มือการปฏิบัติงานสำหรับระบบ

๓.๓ ข้อมูลในฐานข้อมูลของระบบงาน (กรณีที่เป็นระบบงาน)

๓.๔ ข้อมูลซอฟต์แวร์ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงานและซอฟต์แวร์อื่นๆ เป็นต้น

๔. กำหนดความถี่ในการสำรองข้อมูลสำหรับระบบเหล่านั้น (ระบบที่มีการเปลี่ยนแปลงข้อมูลบ่อยควรมีความถี่ในการสำรองข้อมูลสูง)

๕.จัดทำและปรับปรุงแผนกู้คืนระบบอย่างน้อยปีละ ๑ ครั้ง

๕. จัดทำหรือปรับปรุงขั้นตอนปฏิบัติในการสำรองและกู้คืนข้อมูล โดยให้มีการปฏิบัติตาม**แนวทางปฏิบัติ สำหรับการสำรองและทดสอบกู้คืนข้อมูล**

๖. ทดสอบแผนกู้คืนระบบอย่างน้อยปีละ ๑ ครั้ง บันทึกผลการทดสอบซึ่งรวมถึงปัญหาที่พบ และนำเสนอผลการทดสอบและแนวทางแก้ไขต่อผู้บังคับบัญชา

๑๒. นโยบายการสร้างความมั่นคงปลอดภัยทางกายภาพสำหรับพื้นที่ที่ต้องการรักษาความมั่นคงปลอดภัย

วัตถุประสงค์

๑. เพื่อควบคุมและจำกัดการเข้าถึงทางกายภาพสำหรับพื้นที่ที่มีความสำคัญ

๒. เพื่อป้องกันทรัพย์สินในพื้นที่ที่มีความสำคัญไม่ให้เกิดความเสียหาย ถูกเข้าถึงโดยไม่ได้รับอนุญาตหรือถูกขโมย

ผู้รับผิดชอบ

ผู้ดูแลระบบ และ/หรือ ผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

การดำเนินการ

๑. ห้ามนำบุคคลภายนอกเข้าไปในห้องเครื่องโดยไม่มีกิจที่จำเป็น

๒. ห้ามใส่รองเท้าเข้าห้องเครื่อง

๓. ห้ามนำอาหาร และเครื่องดื่มเข้าไปในบริเวณห้องเครื่อง

๔. สำรวจและติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) เพิ่มเติมความจำเป็น เช่น ในกรณีที่เป็นมุมอับ รวมทั้งตรวจสอบการทำงานของกล้องให้มีการทำงานอย่างถูกต้อง ต่อเนื่อง และให้สามารถเก็บภาพได้ในมุมกว้าง และไม่มีสิ่งกีดขวาง

๕. บันทึกและจัดเก็บภาพของกล้องโทรทัศน์วงจรปิดไว้ตามความจะเป็น (เช่น เก็บไว้อย่างน้อย ๑ เดือน) เพื่อใช้ในการตรวจสอบในภายหลัง

๖. ตรวจสอบประตูทางเข้า-ออกและหน้าต่างของห้องเครื่องให้ปิดล็อค (Lock) อยู่เสมอ

๗. จัดให้มีการระมัดระวัง สอดส่องและดูแลการส่งมอบทรัพย์สินสารสนเทศโดยให้ผู้ให้บริการภายนอกจนกระทั่งเสร็จสิ้นงาน

๘. ตรวจสอบ และปรับปรุงข้อมูลรายชื่อผู้มีสิทธิเข้า-ออกห้องเครื่องให้มีความถูกต้องและทันสมัยอย่างน้อยปีละ ๑ ครั้ง

๙. ตรวจสอบห้องสายสัญญาณสื่อสารให้มีการปิดล็อค (Lock) อยู่เสมอ

๑๐. ตรวจสอบตู้ Rack คอมพิวเตอร์ให้มีการปิดล็อค (Lock) อยู่เสมอ

๑๑. ให้ดูแลความสะอาด และความเป็นระเบียบเรียบร้อยของห้องคอมพิวเตอร์แม่ข่ายกลางอย่างสม่ำเสมอ

๑๒. จัดทำและปรับปรุงผังพื้นที่ห้องคอมพิวเตอร์แม่ข่ายกลางให้ทันสมัย อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมจำเป็น

๑๓. นโยบายการป้องกันภัยคุกคามทางด้านสิ่งแวดล้อม

วัตถุประสงค์

เพื่อป้องกันภัยคุกคามทางด้านสิ่งแวดล้อม เช่น ไฟไหม้ น้ำท่วม หรืออื่นๆ ซึ่งอาจเป็นผลให้เกิดความเสียหายต่อทรัพย์สินสารสนเทศของสำนักงาน

ผู้รับผิดชอบ

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

อ้างอิงมาตรฐาน

หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

การดำเนินการ

๑. จัดให้มีการตรวจสอบการทำงานของอุปกรณ์ดับเพลิงอย่างน้อยปีละ ๑ ครั้ง ว่ายังใช้งานได้เป็นปกติหรือไม่

๒. จัดให้มีการประเมินสภาพแวดล้อมของห้องคอมพิวเตอร์แม่ข่ายกลางอย่างน้อยปีละ ๑ ครั้ง และจัดให้มีการปรับปรุงตามความจำเป็น

๑๔. นโยบายการป้องกันระบบ อุปกรณ์และสายสัญญาณต่าง ๆ

วัตถุประสงค์

เพื่อป้องกันระบบ อุปกรณ์ และสายสัญญาณต่างๆ ให้มีความปลอดภัยและสามารถทำงานได้อย่างต่อเนื่องไม่ติดขัด

ผู้รับผิดชอบ

ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

การดำเนินการ

๑. จัดวางเครื่องคอมพิวเตอร์ อุปกรณ์สื่อสาร หรือทรัพย์สินอื่นๆไว้ในบริเวณที่มีความปลอดภัยระมัดระวังการจัดตั้งอุปกรณ์ให้อยู่ในสภาพที่มั่นคง และไม่ล้ม หรือโอนเอียงได้โดยง่าย

๒. ตรวจสอบและบำรุงรักษาห้องคอมพิวเตอร์แม่ข่ายกลาง อุปกรณ์เครือข่าย หรือทรัพย์สินอื่นๆ ที่มีความสำคัญอย่างสม่ำเสมอ

๓. ต่อสัญญาการบำรุงรักษาห้องคอมพิวเตอร์แม่ข่ายกลาง เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ UPS เครื่องปรับอากาศ และอุปกรณ์เครือข่ายที่มีความสำคัญให้ครบถ้วน

๔. จัดให้ระบบงาน เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ที่มีความสำคัญ ต้องมีระบบกระแสไฟฟ้าสำรองสนับสนุนการทำงานอย่างครบถ้วน

๕. ในการเดินสายสัญญาณสื่อสารแบบถาวร ต้องเดินสายอย่างเป็นระเบียบเรียบร้อย ไม่เกะกะขวางทาง และมีการร้อยสายเข้าไปในท่อเพื่อป้องกันความเสียหาย

๖. ตรวจสอบ และจัดเก็บสายสัญญาณสื่อสารให้อยู่ในสภาพที่เป็นระเบียบเรียบร้อย พร้อมทั้งจัดทำลาเบล (Label) ของสายสัญญาณเหล่านั้นให้ครบถ้วน

๗. สถานภาพการทำงานของอุปกรณ์สนับสนุนการทำงานของระบบคอมพิวเตอร์ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ ได้แก่

๗.๑ ระบบกระแสไฟฟ้า

๗.๒ ระบบการระบายอากาศ

๗.๓ ระบบการปรับอุณหภูมิ

๗.๔ ระบบกระแสไฟฟ้าสำรอง เป็นต้น

๑๕. นโยบายการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี ๒๕๕๐

วัตถุประสงค์

๑. เพื่อให้มีการปฏิบัติที่สอดคล้องกับกฎหมาย พ.ร.บ. หรือข้อบังคับภายนอกอื่นๆ ที่ได้กำหนดไว้

๒. เพื่อจำกัดการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์(Log) โดยผู้ที่รับผิดชอบเท่านั้น

ผู้รับผิดชอบ

ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๑๑ การปฏิบัติตามข้อกำหนด

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

การกำหนดการ

๑. จัดเก็บและสำรองข้อมูลจราจรทางคอมพิวเตอร์(Log) ของระบบดังต่อไปนี้ อย่างน้อยเป็นระยะเวลา ๑๘๐ วัน

ชนิดของระบบ	ข้อมูลจราจรฯที่ต้องเก็บ
FTP Server	ข้อมูลจราจรฯที่เกิดจากการโอนย้ายไฟล์
Firewall/Proxy/Gateway	ข้อมูลไอพีแอดเดรสของเครื่องทั้งภายในและภายนอกที่มีการเชื่อมต่อกับเครือข่ายของสำนักงาน
Authentication	ข้อมูลจราจรฯการพิสูจน์ตัวตนของผู้ใช้งาน
Web Server	ข้อมูลจราจรฯการเข้าถึงเว็บเซิร์ฟเวอร์
Web Application	ข้อมูลจราจรฯการพิสูจน์ตัวตนของผู้ใช้งาน

๒. จำกัดการเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ (Log) ดังกล่าวโดยกำหนดสิทธิให้เฉพาะผู้ดูแลระบบที่เกี่ยวข้องเท่านั้นที่สามารถเข้าถึงได้

๑๖. นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless)

วัตถุประสงค์

เพื่อให้การบริหารจัดการระบบเครือข่ายไร้สาย (Wireless) ของสำนักงานมีความเหมาะสม ปลอดภัยและเป็นไปตามกฎหมาย และเพื่อให้ผู้ใช้งานสามารถนำไปใช้ประโยชน์ในการสนับสนุนการปฏิบัติงานตามภารกิจได้อย่างมั่นคงปลอดภัยและไม่ขัดต่อกฎหมาย

ผู้รับผิดชอบ

ผู้ดูแลระบบ/ผู้ใช้งาน

อ้างอิงมาตรฐาน

หมวด ๕ การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

หมวด ๗ การควบคุมการเข้าถึง

หมวด ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสำนักงาน

การดำเนินงานการ

๑. ผู้ดูแลระบบ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๒. ผู้ดูแลระบบ ควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำ อุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๓. ผู้ดูแลระบบ ต้องกำหนดว่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์ กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๔. ผู้ดูแลระบบ ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) หรือ ชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) หรือชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๕. ผู้ดูแลระบบ ควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

๖. ผู้ดูและระบบ ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ รายงานต่อผู้บังคับบัญชาให้ทราบทันที

๗. ผู้ใช้งานที่มีความประสงค์จะใช้งานระบบเครือข่ายไร้สาย (Wireless) จะต้องกรอกแบบฟอร์มการขอใช้งานระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน และนำเสนอต่อผู้บังคับบัญชาเพื่อขออนุมัติใช้งาน เมื่อได้รับการอนุมัติแล้วให้ส่งต่อผู้บังคับบัญชาของผู้ดูแลระบบเพื่อดำเนินการต่อไป

ส่วนที่ ๔
นโยบายการจัดการด้านบุคลากร
สำหรับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

นโยบายการจัดการด้านบุคลากร

วัตถุประสงค์

๑. เพื่อให้มีการกำหนดหน้าที่ความรับผิดชอบที่ชัดเจนสำหรับบุคลากรที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ

๒. เพื่อให้มีการคัดเลือกบุคลากรด้านสารสนเทศที่มีคุณสมบัติเหมาะสมเพื่อมาปฏิบัติหน้าที่ให้กับสำนักงาน

๓. เพื่อให้มีกำหนดเงื่อนไขการจ้างงานบุคลากรที่รัดกุมและเป็นผลประโยชน์ต่อสำนักงาน

๔. เพื่อให้มีการถอดถอนสิทธิของบุคลากรที่ลาออกหรือย้ายไปอยู่แผนกอื่น รวมทั้งตรวจสอบทรัพย์สินของสำนักงานที่ใช้งานโดยเจ้าหน้าที่นั้นก่อนลาออกไป

ผู้รับผิดชอบ

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

อ้างอิงมาตรฐาน

หมวดที่ ๔ ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร

การดำเนินการ

๑. จัดทำและปรับปรุงหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ

๒. เมื่อมีการลาออกหรือย้ายแผนกของเจ้าหน้าที่ ให้ฝ่ายบริหารทั่วไปแจ้งให้กลุ่ม/ฝ่ายที่เกี่ยวข้องได้รับทราบภายใน ๑ สัปดาห์ นับจากมีคำสั่งให้ลาออกหรือย้ายแผนก เพื่อให้ดำเนินการปรับปรุงหรือถอดถอนสิทธิตามความจำเป็น

ส่วนที่ ๕
นโยบายการเผยแพร่ข้อมูลสู่สาธารณะ
สำหรับผู้เป็นเจ้าของหรือรับผิดชอบต่อข้อมูลที่ต้องทำการเผยแพร่สู่สาธารณะ

นโยบายการนำข้อมูลเผยแพร่สู่สาธารณะ

วัตถุประสงค์

เพื่อป้องกันความผิดพลาดของข้อมูลที่จะมีการนำเผยแพร่สู่สาธารณะ ซึ่งอาจก่อให้เกิดความเสียหายต่อชื่อเสียงและภาพลักษณ์ของสำนักงาน

ผู้รับผิดชอบ

ผู้เป็นเจ้าของข้อมูลและผู้มีหน้าที่รับผิดชอบต่อข้อมูลที่ต้องการเผยแพร่สู่สาธารณะ

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

การดำเนินการ

๑. ให้ผู้ที่เป็นเจ้าของข้อมูลซึ่งต้องการนำข้อมูลนั้นขึ้นเผยแพร่สู่สาธารณะและผู้ที่มีหน้าที่รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ของสำนักงานจะต้องทำการตรวจสอบความถูกต้องและเหมาะสมของเนื้อหาก่อน หากมีความผิดพลาดเกิดขึ้นกับเนื้อหาจะต้องรับผิดชอบต่อความผิดพลาดนั้น

๒. ให้ผู้ที่มีหน้าที่รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะ เช่น โดยผ่านทางเว็บไซต์ของสำนักงาน จะต้องดำเนินการด้วยตนเอง หากมีการมอบหมายให้ผู้อื่นดำเนินการแทนต้องทำการตรวจสอบความถูกต้องและเหมาะสมของเนื้อหาโดยทันที เมื่อเผยแพร่ข้อมูลแล้วเสร็จ

ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบงาน

วัตถุประสงค์

เพื่อลดความผิดพลาดในการดำเนินการเปลี่ยนแปลงต่อระบบงาน ซึ่งอาจส่งผลให้ระบบเสียหาย ทำงานผิดปกติ หยุดชะงักการทำงาน หรือไม่สามารถให้บริการได้

ผู้รับผิดชอบ

ผู้บังคับบัญชาของผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๘ การจัดทำ การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

ขั้นตอนปฏิบัติ

๑. เมื่อผู้ใช้ต้องการพัฒนาระบบงานใหม่ปรับปรุง เปลี่ยนแปลง หรือแก้ไขระบบงานเดิมให้มีการกรอกแบบคำขออนุมัติดำเนินการเปลี่ยนแปลงระบบงาน

๒. จัดหมวดหมู่ของการอนุมัติการเปลี่ยนแปลงนั้นว่าเป็นการเปลี่ยนแปลงชนิดใด ซึ่งประกอบด้วย

๒.๑ การพัฒนาระบบงานใหม่

๒.๒ การปรับปรุงระบบงานเดิม

๒.๓ การแก้ไขข้อผิดพลาดในระบบงาน

๓. ประเมินผลกระทบของการเปลี่ยนแปลงนั้นว่ามีผลกระทบมาก (Major) หรือน้อย (Minor) โดยใช้เกณฑ์ดังนี้

๓.๑ ในกรณีที่เป็นการพัฒนาระบบงานใหม่ ให้พิจารณาว่ามีผลกระทบมาก

๓.๒ ในกรณีที่เป็นการปรับปรุงระบบงานเดิมที่ต้องพัฒนาเพิ่มเติม

- ไม่เกินร้อยละ ๑๐ ให้พิจารณาว่ามีผลกระทบน้อย
- เกินกว่าร้อยละ ๑๐ ให้พิจารณาว่ามีผลกระทบมาก

๓.๓ ในกรณีที่เป็นการแก้ไขข้อผิดพลาดในระบบงาน

- การแก้ไขค่อนข้างซับซ้อนและมีปริมาณงานมาก ให้พิจารณาว่ามีผลกระทบมาก
- กรณีอื่นๆ ให้พิจารณาว่ามีผลกระทบน้อย

สำหรับการเปลี่ยนแปลงที่มีผลกระทบมาก (ยกเว้นการพัฒนาระบบงานใหม่) ให้จัดเตรียมแผนถอยหลังกลับด้วย (ในกรณีที่ทำไม่สำเร็จ จะได้กลับไปใช้เวอร์ชั่น (Vision) ก่อนการเปลี่ยนแปลงได้)

๔. ประเมินความเร่งด่วนว่ามีความเร่งด่วน (Urgent) หรือปกติ (Normal) โดยใช้เกณฑ์ดังนี้

๔.๑ ในกรณีที่เป็นการพัฒนาระบบงานใหม่ ให้พิจารณาว่าปกติ

๔.๒ ในกรณีที่เป็นการปรับปรุงระบบงานเดิม และระบบงานนั้นสอดคล้องกับโครงการตามแผนกลยุทธ์สำหรับปีงบประมาณนั้น ให้พิจารณาว่ามีความเร่งด่วนกรณีอื่น ๆ ให้พิจารณาว่าปกติ

๔.๓ ในกรณีที่เป็นการแก้ไขข้อผิดพลาดในระบบงาน

- หากไม่ดำเนินการโดยทันที ระบบจะทำงานผิดพลาดหรือไม่สามารถทำงานได้ให้พิจารณาว่ามีความเร่งด่วน

- กรณีอื่น ๆ ให้พิจารณาว่าปกติ

๕. อนุมัติการขอดำเนินการนั้น

๖. จัดลำดับความสำคัญว่าการขออนุมัติใดที่ต้องทำก่อนหลังเรียงตามลำดับ

๗. จัดให้ทีมผู้พัฒนาระบบวางแผนดำเนินการพัฒนาหรือปรับปรุงระบบงาน

๘. บันทึกข้อมูลข้างต้นทั้งหมดลงใน**แบบคำขออนุมัติดำเนินการเปลี่ยนแปลงระบบงาน** และเมื่อทีมผู้พัฒนาระบบได้ดำเนินการแล้วเสร็จจะต้องบันทึกข้อมูลต่อท้ายแบบคำขออนุมัติฯ ดังกล่าวในส่วนการปฏิบัติด้วย

แนวทางปฏิบัติในการตรวจข้อมูลนำเข้า

วัตถุประสงค์

เพื่อให้ระบบงานได้รับการพัฒนาให้ประมวลผลหรือคำนวณได้อย่างถูกต้อง และเพื่อให้ข้อมูลนำเข้าและนำออกจากระบบมีความถูกต้องและเชื่อถือได้ รวมทั้งปลอดภัยจากการถูก บุกรุก หรือเจาะระบบโดยผู้ไม่ประสงค์ดี

ผู้รับผิดชอบ

ผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

แนวทางปฏิบัติ

๑. ตรวจสอบข้อมูลนำเข้าดังนี้

๑.๑ ตรวจสอบให้ตรงกับชนิดของข้อมูลของตัวแปรของโปรแกรม

๑.๒ ตรวจสอบให้อยู่ภายในช่วงของค่าของตัวแปรของโปรแกรม

๑.๓ ตรวจสอบให้อยู่ภายในค่าขอบเขตบนและล่างของตัวแปรของโปรแกรม

๑.๔ ตรวจสอบเพื่อป้องกันไม่ให้อยู่นอกช่วงของค่าที่กำหนดไว้

๑.๕ ตรวจสอบเพื่อป้องกันข้อมูลขาดหายหรือไม่ครบถ้วน

๑.๖ ตรวจสอบเพื่อป้องกันการใส่ตัวอักษรไม่ถูกต้อง

๑.๗ ตรวจสอบเพื่อป้องกันการลืมใส่ค่าคีย์ (Key) หรือไม่ให้ (Key) มีความซ้ำซ้อนกัน

๑.๘ ตรวจสอบข้อมูลนำเข้าเพื่อป้องกันการใส่ตัวอักษรพิเศษต่าง ๆ

๒. ปฏิบัติตามการตรวจสอบข้อมูลนำเข้าเพื่อป้องกันปัญหา SQL Injection และ Buffer Overflows

๓. จัดให้ระบบงานจัดการกับความผิดพลาดที่เกิดขึ้นจากข้อมูลนำเข้า เช่น ต้องแสดงข้อผิดพลาดเพื่อให้ผู้ใช้งานตรวจสอบและแก้ไขได้

แนวทางปฏิบัติในการตรวจสอบความถูกต้องของการประมวลผลข้อมูล

วัตถุประสงค์

เพื่อให้ระบบงานให้การพัฒนาให้ประมวลผลหรือคำนวณได้อย่างถูกต้อง และเพื่อให้ข้อมูลนำออกจากระบบมีความถูกต้องและเชื่อถือได้

ผู้รับผิดชอบ

ผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

แนวทางปฏิบัติ

๑. ปฏิบัติตามการตรวจสอบความถูกต้องของการประมวลผลข้อมูลดังนี้

๑.๑ ในระหว่างที่พัฒนาระบบงาน ให้ตรวจสอบ

- ค่าตัวแปรของโปรแกรม หลังจากที่มีการเรียกใช้ฟังก์ชั่น (Function) เสร็จสิ้น
- ผลการประมวลผล การคำนวณ หรือผลรวมในตัวแปรอย่างเป็นระยะ ๆ ว่าค่าที่ได้รับมีความถูกต้องหรือไม่ ถ้าไม่ถูกต้อง ให้ตรวจสอบหาสาเหตุและดำเนินการแก้ไข

๑.๒ บันทึกค่าของตัวแปรหรือผลการประมวลผลเหล่านั้นไว้ หลังจากนั้นให้ตรวจสอบความถูกต้อง ถ้าไม่ถูกต้อง ให้ตรวจสอบหาสาเหตุและดำเนินการแก้ไข

มาตรฐานทางด้านความมั่นคงปลอดภัยในการพัฒนาระบบงาน

วัตถุประสงค์

เพื่อกำหนดมาตรฐานขั้นต่ำของการพัฒนาระบบงานเพื่อให้ระบบงานมีความมั่นคงปลอดภัยจากการถูกเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต หรือจากการถูกบุกรุกระบบ

ผู้รับผิดชอบ

ผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๗ การควบคุมการเข้าถึง

หมวดที่ ๘ การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

การดำเนินการ

๑. ให้ระบบข้อกำหนดทางด้านความมั่นคงปลอดภัย (Security Requirement) ในการพัฒนาระบบงานเช่น การเข้ารหัสข้อมูลที่มีการรับส่งระหว่างเครื่องลูกข่ายกับเครื่องแม่ข่าย การกำหนดสิทธิ์ในการใช้งานตามความจำเป็น การกำหนดให้ผู้ใช้งานมีการตั้งรหัสผ่านที่มีความเข้มแข็ง เป็นต้น

๒. ให้พัฒนาระบบงานเพื่อให้มีหน้าจอสำหรับผู้ดูแลระบบงานให้สามารถบันทึก และปรับปรุงสิทธิของผู้ใช้งานได้ รวมทั้งต้องสามารถบันทึกสิทธิดังกล่าวลงเก็บไว้ในฐานข้อมูลได้ด้วย

๓. ให้พัฒนาระบบงานเพื่อให้ผู้ใช้งานสามารถกำหนดรหัสผ่านที่มีความปลอดภัยตามนโยบาย การตั้งรหัสผ่าน ได้แก่การกำหนดความยาวและระยะเวลาการเปลี่ยนรหัสผ่าน

๔. ให้พัฒนาระบบงาน ให้การล็อกอิน (Login) ของผู้ใช้เข้าสู่ระบบงานมีความปลอดภัย โดยปฏิบัติตามแนวทางดังนี้

๔.๑ ไม่แสดงรายละเอียดของระบบจนกว่าจะล็อกอิน (Login) สำเร็จ

๔.๒ ไม่มีหรือไม่แสดงฟังก์ชั่น (Function) ให้การช่วยเหลือในระหว่างที่ทำการล็อกอิน (Login)

๔.๓ บันทึกความพยายามในการล็อกอิน (Login) ทั้งที่สำเร็จและไม่สำเร็จและแสดงประวัติการล็อกอิน (Login) ๓ ครั้งล่าสุด

๔.๔ ตัดการเชื่อมต่อหลังจากทำการล็อกอิน (Login) ไม่สำเร็จเกินกว่า ๓ ครั้ง

๔.๕ เมื่อมีการใส่บัญชีผู้ใช้งานและรหัสผ่านที่ไม่ถูกต้อง ให้แสดงข้อความรวม ๆ เช่น “ข้อมูลการล็อกอิน (Login) ไม่ถูกต้อง”

๔.๖ ให้แสดงข้อความเตือนที่หน้าจอภายหลังจากการล็อกอิน (Login) เสร็จสิ้น ข้อความเตือนดังกล่าวได้แก่ “ระบบนี้เป็นระบบที่เป็นทรัพย์สินของสำนักงาน การใช้งานจะต้องได้รับการอนุมัติก่อนเท่านั้นจึงจะสามารถใช้งานได้ ผู้ที่ไม่ได้รับสิทธิและเข้ามาใช้ระบบงาน หากมีการตรวจพบอาจมีการลงโทษทางวินัย หรือดำเนินการทางกฎหมายตามความเหมาะสม สำนักงานมีสิทธิในการตรวจสอบพฤติกรรมการใช้งานในระหว่างที่ผู้ใช้ใช้ระบบงานนี้”

ขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี

วัตถุประสงค์

เพื่อให้มีการบริหารจัดการปัญหาไวรัส และดำเนินการแก้ไขได้อย่างเหมาะสม ได้ผลและทันกาล

ผู้รับผิดชอบ

ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศ ของสำนักงาน

หมวดที่ ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ของสำนักงาน

ขั้นตอนปฏิบัติ

เมื่อผู้รับผิดชอบได้รับแจ้งจากผู้ใช้เกี่ยวกับปัญหาไวรัส ให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

๑. ดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ในเบื้องต้นด้วยโปรแกรมป้องกันไวรัสว่าเครื่องคอมพิวเตอร์นั้นติดไวรัสหรือไม่

๒. หากพบว่ามีไวรัสให้ตัดการเชื่อมต่อเครื่องดังกล่าวออกจากระบบเครือข่าย เช่น ถอดสาย LAN ออก

๓. หากทราบชื่อของไวรัสนั้น ให้เข้าไปที่เว็บไซต์ของผู้ผลิตซอฟต์แวร์ (Software) ป้องกันไวรัสที่สำนักงานใช้งานเพื่อศึกษาข้อมูลวิธีการการแก้ไขหรือดูข้อมูลเพิ่มเติมจากเว็บของ ThaiCERT รวมทั้งให้ทำการดาวน์โหลด (Download) เครื่องมือหรือทูล (Tool) ต่าง ๆ ที่จำเป็นสำหรับการแก้ไข

๔. ศึกษาและวิเคราะห์การทำงานของไวรัสนั้น เช่น มี โปรเซส (Process) แปลกปลอมอะไรบ้างที่ทำงานอยู่ มีไฟล์แปลกปลอมเพิ่มเติมอะไรบ้าง เป็นต้น

๕. ตรวจสอบว่ามีไฟล์ใดบ้างในเครื่องที่ได้รับความเสียหาย เพื่อเตรียมการติดตั้งหรือกู้คืนไฟล์ดังกล่าว

๖. ในกรณีที่มี Process แปลกปลอมทำงานอยู่ ให้หยุดการทำงานของ Process นั้น

๗. ติดตั้ง Patch หรือใช้เครื่องมือฟิกทูล (Fix Tool) ตามคำแนะนำของผู้ผลิตซอฟต์แวร์ (Software) ป้องกันไวรัสเพื่อทำการแก้ไขเครื่อง

๘. สำหรับไฟล์ที่เสียหาย ให้นำข้อมูลที่สำรองไว้มาติดตั้งกลับคืน

๙. หาก Process ที่ได้หยุดการทำงานไว้นั้น มีความจำเป็นต้องใช้งาน ให้เปิดการทำงาน Process นั้นใหม่อีกครั้ง

๑๐. เชื่อมโยงเครื่องคอมพิวเตอร์ที่ได้รับการแก้ไขแล้วกลับคืนสู่เครือข่ายเพื่อให้ใช้งานได้ตามปกติ

๑๑.แจ้งให้ผู้ที่เกี่ยวข้องทราบถึงการแก้ไขปัญหาที่ได้ดำเนินการไป รวมทั้งให้คำแนะนำในการระมัดระวังและป้องกันไวรัส

๗. นโยบายการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย

ขั้นตอนปฏิบัติสำหรับการจัดการกับเหตุการณ์ด้านความมั่นคงปลอดภัย

วัตถุประสงค์

เพื่อให้มีการบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย และดำเนินการแก้ไขได้อย่างเหมาะสมได้ผลและทันกาล

ผู้รับผิดชอบ

ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๙ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสำนักงาน

ขั้นตอนปฏิบัติ

เมื่อผู้รับผิดชอบได้รับแจ้งจากผู้ใช้เกี่ยวกับเหตุการณ์ทางด้านความมั่นคงปลอดภัย ให้ปฏิบัติตามขั้นตอนดังต่อไปนี้

๑. ประเมินผลกระทบของเหตุการณ์ที่เกิดขึ้น โดยอ้างอิงตามเกณฑ์ตามแนวทางการบริหารความเสี่ยงของสำนักงาน

๒. แจ้งให้ผู้บังคับบัญชาตามลำดับชั้นได้รับทราบ เฉพาะกรณีที่เหตุการณ์นั้นมีผลกระทบตั้งแต่ระดับปานกลาง (Medium) ขึ้นไป

๓. ดำเนินการตามความจำเป็น ตามประเภทของเหตุการณ์ดังนี้

๓.๑ สำหรับเหตุการณ์ด้านระบบถูกบุกรุกหรือโจมตี ให้ขอความช่วยเหลือจาก ThaiCERT ในการวิเคราะห์เหตุการณ์และดำเนินการแก้ไข

๓.๒ สำหรับเหตุการณ์หน้าเว็บไซต์หลักของสำนักงานถูกเปลี่ยน ให้รายงานผู้บังคับบัญชาของผู้ดูแลระบบเพื่อขอความเห็นในการดำเนินการ รวมทั้งอาจขอความช่วยเหลือจาก ThaiCERT ในการวิเคราะห์และดำเนินการแก้ไข

๓.๓ สำหรับเหตุการณ์บุกรุกทางกายภาพของห้องคอมพิวเตอร์แม่ข่ายกลาง ให้รายงานผู้บังคับบัญชาของผู้ดูแลระบบ เพื่อขอความเห็นในการดำเนินการแก้ไข

๓.๔ สำหรับเหตุการณ์ซอฟต์แวร์มีจุดอ่อนหรือทำงานผิดปกติ ให้รายงานผู้บังคับบัญชาของผู้พัฒนาระบบและ/หรือผู้ดูแลระบบ เพื่อขอความเห็นในการดำเนินการแก้ไข

๓.๕ สำหรับเหตุการณ์ไม่ปฏิบัติตามนโยบายความมั่นคงปลอดภัยและเหตุการณ์ที่เกี่ยวข้องอื่นๆ ให้รายงานผู้บังคับบัญชาผู้ดูแลระบบและ/หรือผู้ดูแลระบบ เพื่อขอความเห็นในการดำเนินการแก้ไข

๔. บันทึกข้อมูลที่เกี่ยวข้องกับเหตุการณ์ดังกล่าวใน**แบบรายงานเหตุการณ์ทางด้านความมั่นคงปลอดภัย**

๕. ทำรายงานสรุปสำหรับเหตุการณ์ที่มีผลกระทบตั้งแต่ระดับปานกลาง (Medium) ขึ้นไปและแจ้งเวียนให้ผู้ที่เกี่ยวข้องได้รับทราบ

โครงสร้างพื้นฐานสารสนเทศที่ควบคุม

โครงสร้างพื้นฐานสารสนเทศที่ต้องควบคุมเมื่อจะดำเนินการติดตั้ง เปลี่ยนแปลง แก้ไข หรือปรับปรุง ประกอบด้วย

๑. ระบบงานสำคัญทั้งหมด

๒. ฮาร์ดแวร์ (Hardware) ของระบบงานสำคัญ

๓. ซอฟต์แวร์ (Software) ต่าง ๆ บนระบบงานสำคัญ ซึ่งรวมถึงระบบปฏิบัติการ ระบบบริหารจัดการฐานข้อมูล การติดตั้งปิดช่องโหว่ (Patch)

๔. ฐานข้อมูลของระบบงานสำคัญ

๕. ไฟร์วอลล์ (Firewall)

๖. เราท์เตอร์ (Router)

๗. ระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS)

ขั้นตอนปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ

วัตถุประสงค์

เพื่อลดความผิดพลาดในการดำเนินการเปลี่ยนแปลงต่อโครงสร้างพื้นฐานสารสนเทศ ซึ่งอาจส่งผลให้ระบบเสียหาย ทำงานผิดปกติ หยุดชะงักการทำงาน หรือไม่สามารถให้บริการได้

ผู้รับผิดชอบ

ผู้บังคับบัญชาของผู้ดูแลระบบ และ/หรือผู้พัฒนาระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

การดำเนินการ

๑. เมื่อผู้ดูแลระบบและ/หรือผู้พัฒนาระบบ ต้องการติดตั้ง เปลี่ยนแปลง แก้ไข หรือปรับปรุง **โครงสร้างพื้นฐานสารสนเทศที่ควบคุม** จัดให้มีการกรอก**แบบคำขอสำหรับควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานสารสนเทศ** เพื่อขออนุมัติดำเนินการเปลี่ยนแปลง

๒. หารือกับผู้ดูแลระบบและ/หรือผู้พัฒนาระบบ เกี่ยวกับการติดตั้งหรือปรับปรุงโครงสร้างพื้นฐานดังกล่าว

๓. จัดหมวดหมู่ของการอนุมัติการเปลี่ยนแปลงนั้นว่าเป็นการเปลี่ยนแปลงชนิดใด ซึ่งประกอบด้วย

๓.๑ การเปลี่ยนแปลงที่เกี่ยวข้องกับระบบงาน

๓.๒ การเปลี่ยนแปลงกับอุปกรณ์เครือข่าย (เช่น ไฟร์วอลล์ (Firewall) เราท์เตอร์ (Router) ระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) เป็นต้น

๔. ประเมินผลกระทบของการเปลี่ยนแปลงนั้นว่ามีผลกระทบมาก (Major) หรือน้อย (Minor) ในกรณีที่เป็นการเปลี่ยนแปลงดังนี้ ให้พิจารณาว่ามีผลกระทบมาก

๔.๑ ติดตั้ง/ปรับปรุงฮาร์ดแวร์ของระบบงานสำคัญ

๔.๒ ติดตั้ง/ปรับปรุงซอฟต์แวร์ต่างๆ บนระบบงานสำคัญ ซึ่งรวมถึงระบบปฏิบัติการ ระบบบริหารจัดการฐานข้อมูล การติดตั้งปิดช่องโหว่ (Patch)

๔.๓ ติดตั้งระบบงานสำคัญ

๔.๔ ปรับปรุงโครงสร้างของฐานข้อมูลของระบบงานสำคัญ

๔.๕ ติดตั้ง/ปรับปรุงไฟล์วอลล์ (Firewall) เราท์เตอร์ (Router) หรือระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS)

สำหรับการเปลี่ยนแปลงอื่นๆ ให้พิจารณาผลกระทบเป็นกรณีไป โดยใช้เกณฑ์ดังนี้

๔.๖ การเปลี่ยนแปลงที่มีขั้นตอนการดำเนินการที่มากหรือซับซ้อน หรือใช้เวลาเกินกว่า 3 ชั่วโมงจึงจะแล้วเสร็จ หรือมีผลกระทบกับผู้ใช้งานเป็นจำนวนมาก ให้พิจารณาว่ามีผลกระทบมาก

๔.๗ กรณีอื่นๆ ให้พิจารณาว่ามีผลกระทบน้อย

สำหรับการเปลี่ยนแปลงที่มีผลกระทบมาก จัดให้ผู้ขอเปลี่ยนแปลงจัดทำแผนการถอยหลังกลับ (ในกรณีที่ทำไม่สำเร็จ จะได้กลับไปใช้เวอร์ชัน (Version) ก่อนการเปลี่ยนแปลงได้)

๕. ประเมินความเร่งด่วนว่ามีความเร่งด่วน (Urgent) หรือปกติ (Normal) โดยใช้หลักเกณฑ์ดังนี้

๕.๑ หากเป็นการเปลี่ยนแปลงที่ต้องดำเนินการภายใน ๒ วันทำการ ซึ่งรวมถึงการเปลี่ยนแปลงที่ต้องทำอย่างฉุกเฉิน เช่น อุปกรณ์/เครื่องแม่ข่ายสำคัญเสีย ให้พิจารณาว่ามีความเร่งด่วน

๕.๒ หากสามารถดำเนินการได้หลังจาก ๒ วันทำการ ให้พิจารณาว่าปกติ

๖. ในกรณีที่เป็นการเปลี่ยนแปลงเร่งด่วน จัดให้ผู้ขอเปลี่ยนแปลงแจ้งผู้บังคับบัญชาของผู้ดูแลระบบ ก่อนเข้าไปทำการเปลี่ยนแปลง หลังจากนั้นจึงทำเอกสารขออนุมัติทำการเปลี่ยนแปลงเข้ามาในภายหลัง

๗. อนุมัติการขอดำเนินการนั้น

๘. จัดลำดับความสำคัญว่าการขออนุมัติใดที่ต้องทำก่อนหลังเรียงตามลำดับ

๙. จัดให้ผู้ขอเปลี่ยนแปลงวางแผนดำเนินการเปลี่ยนแปลงนั้น

๑๐. บันทึกข้อมูลข้างต้นทั้งหมดลงในแบบคำขออนุมัติเปลี่ยนแปลง

แนวทางปฏิบัติ สำหรับการสำรองและการกู้คืนข้อมูล

วัตถุประสงค์

เพื่อให้มีการปฏิบัติเพื่อสำรองข้อมูลของระบบต่างๆ รวมทั้งทดสอบข้อมูลที่สำรองไว้นั้นอย่างสม่ำเสมอ

ผู้รับผิดชอบ

ผู้ดูแลระบบ

อ้างอิงมาตรฐาน

หมวดที่ ๖ การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศของสำนักงาน

แนวทางปฏิบัติ

๑. สำรองข้อมูลตามความถี่ที่กำหนดไว้

๒. ตรวจสอบว่าการสำรองข้อมูลที่เกิดขึ้นนั้นสำเร็จครบถ้วนหรือไม่ หากไม่สำเร็จ ให้หาสาเหตุ ดำเนินการแก้ไข และดำเนินการใหม่อีกครั้งหนึ่ง

๓. นำข้อมูลที่สำรองไว้นั้นไปเก็บไว้ทั้งในและนอกสถานที่อย่างน้อยอย่างละ ๑ ชุด

๔. ทดสอบกู้คืนข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ (เช่นปีละ ๑ ครั้ง) เพื่อดูว่าข้อมูลยังคงสามารถใช้งานได้ตามปกติหรือไม่

-ꙮꙮ-