ประกาศองค์การตลาดเพื่อเกษตรกร

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศองค์การตลาดเพื่อเกษตรกร

พ.ศ. ๒๕๖๗

เพื่อให้ระบบเทคโนโลยีสารสนเทศขององค์การตลาดเพื่อเกษตรกร เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่องค์การตลาดเพื่อเกษตรกร และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขึ้น

อาศัยอำนาจตามความในมาตรา ๒๑ (๒) แห่งพระราชกฤษฎีกาจัดตั้งองค์การตลาดเพื่อเกษตรกร พ.ศ. ๒๕๑๗ ผู้อำนวยการองค์การตลาดเพื่อเกษตรกรจึงออกประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศองค์การตลาดเพื่อเกษตรกร เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศองค์การตลาดเพื่อเกษตรกร พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“อ.ต.ก.” หมายความว่า องค์การตลาดเพื่อเกษตรกร

“ผู้บริหาร” หมายความว่า ผู้อำนวยการ อ.ต.ก. และพนักงานตำแหน่งบริหารตั้งแต่ระดับ ๘ ขึ้นไป

“พนักงาน” หมายความว่า พนักงานและลูกจ้างของ อ.ต.ก.

“ผู้ใช้งาน” หมายความว่า ผู้บริหาร พนักงาน และผู้ใช้งานที่ได้รับอนุญาตให้เข้าถึงการใช้งานระบบสารสนเทศและระบบเครือข่ายของ อ.ต.ก. และให้หมายรวมถึงบุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. ด้วย

ข้อ ๔ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของ อ.ต.ก. มีวัตถุประสงค์ดังต่อไปนี้

(๑) เพื่อให้มีการเข้าถึงหรือควบคุมการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. ได้แก่ ระบบสารสนเทศ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย การบริการระบบงานอุปกรณ์เครือข่าย และอุปกรณ์คอมพิวเตอร์อื่นๆ ตลอดจนการบริหารจัดการและแก้ไขปัญหาหรือความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศและระบบเครือข่ายของ อ.ต.ก. เป็นไปอย่างมั่นคงปลอดภัย

(๒) เพื่อเผยแพร่ให้ ผู้ใช้งานได้รับทราบเพื่อสร้างความเข้าใจ ความตระหนัก และการมีส่วนร่วมในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๓) ให้มีการเตรียมความพร้อมของการใช้งานสารสนเทศและระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. อย่างต่อเนื่อง โดยการจัดทำแผนและขั้นตอนการปฏิบัติงานกรณีเหตุฉุกเฉิน และการจัดให้มีระบบสำรองให้สามารถรับมือกับกรณีเกิดเหตุฉุกเฉินและเพื่อให้สามารถกู้คืนระบบกลับมาได้ภายในระยะเวลาที่เหมาะสม

(๔) เพื่อใช้เป็นกรอบมาตรฐานและแนวทางปฏิบัติด้านสารสนเทศสำหรับพนักงานของ อ.ต.ก. และผู้ใช้งานถือปฏิบัติอย่างเคร่งครัด

/(๕) เพื่อติดตาม...

(๕) เพื่อติดตาม ตรวจสอบ ประเมินความเสี่ยง และทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศให้เป็นปัจจุบัน ซึ่งสอดคล้องกับสภาพแวดล้อม มาตรฐาน และกฎหมายที่เกี่ยวข้องอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสม

(๖) ให้มีการรักษาไว้ซึ่งความลับ ความถูกต้อง ความสมบูรณ์ และความพร้อมใช้ของสารสนเทศและระบบเทคโนโลยีสารสนเทศของ อ.ต.ก.

ข้อ ๕ เพื่อให้การปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของ อ.ต.ก. ตามข้อ ๔ ได้ดำเนินการให้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล และสามารถปฏิบัติตามได้อย่างเป็นรูปธรรม อ.ต.ก. จึงกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขึ้นตามเอกสารแนบท้ายประกาศนี้ เพื่อให้ผู้ใช้งานปฏิบัติตามโดยเคร่งครัด ทั้งนี้ ประกอบด้วยเนื้อหาดังต่อไปนี้

(๑) การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
(๒) การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ
(๓) การควบคุมการเข้าถึง
(๔) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
(๕) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร
(๖) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
(๗) การจัดหาและพัฒนาระบบเทคโนโลยีสารสนเทศ
(๘) การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ
(๙) การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
(๑๐) การบริหารจัดการผู้ให้บริการภายนอก
(๑๑) การป้องกันโปรแกรมไม่ประสงค์ดี
(๑๒) การรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ท
(๑๓) การประเมินความเสี่ยง
(๑๔) การกำหนดผู้รับผิดชอบ
(๑๕) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

ข้อ ๖ ผู้ใช้งานต้องปฏิบัติตามประกาศนี้และเอกสารแนบท้ายตามประกาศนี้อย่างเคร่งครัด

ประกาศ ณ วันที่ ๒๗ สิงหาคม พ.ศ. ๒๕๖๗

(นายพีรพันธ์ คอทอง)
อธิบดีกรมส่งเสริมการเกษตร
ประธานกรรมการองค์การตลาดเพื่อเกษตรกร

เอกสารแนบท้าย

ประกาศองค์การตลาดเพื่อเกษตรกร

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศองค์การตลาดเพื่อเกษตรกร

องค์การตลาดเพื่อเกษตรกร
WWW.ORTORKOR.COM

แนวปฏิบัติ
การรักษาความมั่นคงปลอดภัยสารสนเทศ
องค์การตลาดเพื่อเกษตรกร
พ.ศ. 2567

กองเทคโนโลยีและสารสนเทศ

สารบัญ

คำนิยาม

๑. **“ความมั่นคงปลอดภัยด้านสารสนเทศ” (Information Seucurity)** หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความครบถ้วนและถูกต้อง (Integity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

๒. **“ระบบเทคโนโลยีสารสนเทศ” (Information Technology System)** หมายถึง ระบบงานที่นำเทคโนโลยีสารสนเทศมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์และเทคโนโลยีการสื่อสารโทรคมนาคม ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) และสารสนเทศ (Information) เป็นต้น

๓. **“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” (Chief Information Officer : CIO)** หมายถึง ผู้ที่มีอำนาจหน้าที่และความรับผิดชอบในการกำกับดูแลการดำเนินงานด้านเทคโนโลยีสารสนเทศและการสื่อสารในองค์กร ด้านการวางระบบเชื่อมโยงข้อมูลภายในองค์กร ระหว่างส่วนราชการและการเชื่อมโยงข้อมูลกับระบบข้อมูลเทคโนโลยีสารสนเทศภาครัฐและการดำเนินงานตามกฎหมายข้อมูลข่าวสาร ได้รับการแต่งตั้งจากผู้อำนวยการ อ.ต.ก.

๓. **“ผู้ดูแลระบบ” (System Administrator)** หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมาย ให้มีหน้าที่รับผิดชอบในการบริหารจัดการการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. ได้แก่ การกำหนดบัญชีรายชื่อผู้ใช้งานการกำหนดสิทธิ์หรือการจำกัดสิทธิ์ให้กับผู้ใช้งานรวมทั้งการดูแลและบำรุงรักษาระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. ให้สามารถใช้งานได้อย่างต่อเนื่อง

๔. **“เจ้าของระบบงาน” (System Owner)** หมายถึง ผู้ซึ่งรับผิดชอบในการดูแลและบำรุงรักษาหรือปรับปรุงระบบงานที่ใช้ใน อ.ต.ก.

๕. **“เจ้าของข้อมูล” (Information Owner)** หมายถึง ผู้ซึ่งรับผิดชอบข้อมูลของ อ.ต.ก. ซึ่งรวมถึง ผู้บังคับบัญชาของเจ้าของข้อมูลนั้นด้วย โดยเจ้าของข้อมูลเป็นผู้ที่รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบ โดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๖. **“ผู้ใช้งาน” (User)** หมายถึง เจ้าหน้าที่ของ อ.ต.ก. หรือบุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. รวมทั้งบุคคลภายนอกที่ได้รับอนุญาต (Authorized User) ให้เข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. โดยมีสิทธิและหน้าที่ในการใช้งานตามที่ อ.ต.ก. กำหนด

๗. **“หน่วยงานภายนอก/ผู้ให้บริการภายนอก/บุคคลภายนอก” (Outside Agency/Service Provider/Third Party)** หมายถึง ลูกค้าหรือผู้ให้บริการภายนอก (Third Party/IT Outsourcing) หรือบุคคลภายนอก ที่ใช้งานระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. ได้เป็นครั้งคราวหรือตามสัญญา

๘. **“สิทธิ์ของผู้ใช้งาน” (User Right)** หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใด ที่เกี่ยวข้องกับการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศของ อ.ต.ก.

๙. **“สินทรัพย์” (Asset)** หมายถึง สิ่งที่มีคุณค่า มีมูลค่า และเป็นทรัพย์สินที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่ อ.ต.ก. เป็นเจ้าของ เช่า ว่าจ้าง พัฒนา หรือจัดซื้อ โดยแบ่งออกเป็นประเภทต่างๆ

ได้ ดังนี้ ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) สารสนเทศ (Information) สื่อบันทึกประเภทพกพา (Removable Media) บริการสาธารณูปโภคพื้นฐาน (Service) และบุคลากร (People)

๙.๑ **“ฮาร์ดแวร์” (Hardware)** หมายถึง อุปกรณ์ต่างๆ ที่ประกอบขึ้นเป็นเครื่องคอมพิวเตอร์ระบบคอมพิวเตอร์ รวมทั้งอุปกรณ์ต่อพ่วงต่างๆ ที่สามารถมองเห็นและสัมผัสได้

๙.๑.๑ **“คอมพิวเตอร์แม่ข่าย” (Server)** หมายถึง เครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นศูนย์กลางของการทำงานในระบบคอมพิวเตอร์ ซึ่งให้บริการแก่เครื่องคอมพิวเตอร์ตามที่ร้องขอ ได้แก่ การประมวลผลข้อมูล การจัดเก็บข้อมูล การป้องกันไวรัส

๙.๑.๒ **“เครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์ลูกข่าย” (Computer or Client Computer)** หมายถึง อุปกรณ์ที่ใช้ในการประมวลผลข้อมูลผ่านซอฟต์แวร์หรือซอฟต์แวร์ประยุกต์ เพื่อให้ได้ผลลัพธ์ตามที่ต้องการ ได้แก่ คอมพิวเตอร์ส่วนบุคคล (Personal Computer) หรือคอมพิวเตอร์แบบพกพาได้ (Notebook Computer) รวมทั้งอุปกรณ์อัจฉริยะ (Smart Device) หรืออุปกรณ์พกพา (Mobile Device)

๙.๑.๓ **“อุปกรณ์ต่อพ่วง” (Peripheral Device)** หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์ เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์สามารถทำงานได้ตามต้องการ ได้แก่ การนำเข้าข้อมูล หรือการแสดงผล

๙.๑.๔ **“สื่อสัญญาณ” (Signal)** หมายถึง สื่อกลางใด ๆ ได้แก่ สายทองแดง สายใยแก้วนำแสง หรือระบบเครือข่ายไร้สาย ทำหน้าที่เชื่อมต่อระหว่างเครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นๆ ในระบบเครือข่าย

๙.๑.๕ **“ระบบเครือข่าย” (Network)** หมายถึง ระบบที่เชื่อมโยงเครื่องคอมพิวเตอร์ หรือระบบเครือข่ายอื่นๆ เข้าด้วยกันเพื่อการติดต่อสื่อสารหรือการแลกเปลี่ยนข้อมูล

๙.๑.๕.๑ **“ระบบอินเตอร์เน็ท” (Internet)** หมายถึง ระบบเครือข่ายที่เชื่อมโยงคอมพิวเตอร์หรือระบบเครือข่ายของ อ.ต.ก. เข้ากับระบบเครือข่ายภายนอกทั่วโลก

๙.๑.๕.๒ **“ระบบอินทราเน็ท” (Intranet)** หมายถึง ระบบเครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์หรือระบบเครือข่ายภายในของ อ.ต.ก. เข้าด้วยกัน

๙.๑.๖ **“ระบบป้องกันการบุกรุก” (Intrusion Protection System)** หมายถึง ระบบรักษาความปลอดภัย ประกอบด้วย ฮาร์ดแวร์หรือซอฟต์แวร์ทำหน้าที่ป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศได้ และจำกัดการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศของผู้ใช้งานภายในให้เป็นไปตามที่กำหนด

๙.๒ **“ซอฟต์แวร์” (Software)** หมายถึง โปรแกรมประเภทหนึ่งที่ถูกสร้างขึ้นสำหรับใช้งานเฉพาะทาง เช่น ระบบ OC ระบบ E-mail เป็นต้น

๙.๓ **“สารสนเทศ” (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจจะอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

๑๐. **“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” (Accessing or Controlling for use of Information)** หมายถึง การอนุมัติ การกำหนดสิทธิ์ การตรวจสอบหรือการมอบอำนาจให้ผู้ใช้งานภายในและ บุคคลภายนอกให้สามารถเข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศของ อ.ต.ก.

๑๑. **“เหตุการณ์ด้านความมั่นคงปลอดภัย” (Information Security Event)** หมายถึง เหตุการณ์ ที่แสดงให้เห็นถึงความเป็นไปได้ที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. จากการละเมิดหรือฝ่าฝืน การปฏิบัติตามแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศหรือความประมาท

๑๒. **“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (Information Security Incident)** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ (Unwanted) หรือไม่อาจคาดคิด (Unexpected) ซึ่งมีแนวโน้มทำให้ระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. ถูกบุกรุก ถูกโจมตีหรือถูกคุกคาม

๑๓. **“ซอฟต์แวร์ไม่ประสงค์ดี” (Malicious Software)** หมายถึง ซอฟต์แวร์ที่ตั้งใจใส่เข้าไปในระบบ เทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต เพื่อให้ทำงานตามความความต้องการของผู้ไม่ประสงค์ดี ส่งผลให้ ระบบเทคโนโลยีสารสนเทศได้รับความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม จนเกิดความ ขัดข้องหรือไม่สามารถปฏิบัติงานได้

๑๔. **“บัญชีรายชื่อ” (User Account)** หมายถึง รายชื่อของผู้ใช้งานที่ได้รับอนุญาตหรือไม่ได้รับอนุญาตให้เข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศของ อ.ต.ก.

๑๔.๑ **“บัญชีรายชื่อผู้ดูแลระบบ” (Administrator Account)** หมายถึง รายชื่อของผู้ดูแลระบบที่ได้รับอนุญาตหรือไม่ได้รับอนุญาตให้เข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศของ อ.ต.ก.

๑๔.๒ **“บัญชีรายชื่อผู้ใช้งาน” (User Account)** หมายถึง รายชื่อของผู้ใช้งานภายในและบุคคลภายนอกที่ได้รับอนุญาตหรือไม่ได้รับอนุญาตให้เข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศของ อ.ต.ก.

๑๔.๓ **“รหัสผ่าน” (Password)** หมายถึง ตัวอักษร อักขระหรือตัวเลขที่ใช้สำหรับตรวจสอบการพิสูจน์ตัวตนหรือการยืนยันตัวตนของผู้ใช้งาน

๑๕. **“การพิสูจน์ตัวตนหรือการยืนยันตัวตน” (Authentication)** หมายถึง ขั้นตอนในการพิสูจน์ ตัวตนของผู้ใช้งานเพื่อควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. โดยทั่วไปแล้วจะ ตรวจสอบรายชื่อผู้ใช้งาน (Username) ร่วมกับรหัสผ่าน (Password) เป็นอย่างน้อย

๑๖. **“พื้นที่ใช้งาน” (Information System Workspace)** หมายถึง พื้นที่ที่อนุญาตให้มีการเข้าถึง และการใช้งานระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. ได้แก่

๑๖.๑ **“พื้นที่ทำงานทั่วไป” (General Working Area)** หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ ส่วนบุคคล และคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน

๑๖.๒ **“พื้นที่ทำงานของผู้ดูแลระบบ” (System Administrator Area)** หมายถึง พื้นที่ควบคุม ที่อนุญาตให้เฉพาะผู้ดูแลระบบที่มีสิทธิ์เท่านั้น

๑๖.๓ **“พื้นที่ติดตั้งอุปกรณ์ของระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย” (IT Equipment or Network Area)** หมายถึง พื้นที่สำหรับติดตั้งอุปกรณ์ที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่าย

๑๖.๔ **“การเข้าถึงระบบเครือข่ายจากระยะไกล” (Remote Access)** หมายถึง การเชื่อมต่อ เครื่องคอมพิวเตอร์หรือระบบเครือข่ายอื่นๆ เข้ากับระบบเครือข่ายของ อ.ต.ก. ผ่านอุปกรณ์สื่อสารหรือสื่อ สัญญาณอื่นๆ ได้แก่ VPN (Virtual Private Network)

๑๖.๕ **“การควบคุมการเข้าถึง” (Access Control)** หมายถึง การควบคุมการเข้าถึงหรือการใช้งานระบบเทคโนโลยีสารสนเทศให้เป็นไปตามสิทธิ์และหน้าที่ของผู้ใช้งานที่กำหนดไว้เท่านั้น

๑๖.๖ **“การเข้ารหัส” (Encryption)** หมายถึง การนำข้อมูลมาผ่านกระบวนการเข้ารหัสเพื่อป้องกันการลักลอบเข้าถึงหรือใช้ข้อมูลโดยผู้ที่ไม่ได้รับอนุญาติโดยผู้ที่ได้รับอนุญาตหรือมีกุญแจถอดรหัสเท่านั้นที่สามารถเข้าถึงหรือใช้ข้อมูลที่เข้ารหัสได้

๑๖.๗ **“เอกสารโครงแบบ” (Configuration Document)** หมายถึง เอกสารที่แสดงรายละเอียดการกำหนดค่าต่างๆ ในระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถทำงานได้ตามความต้องการ

๑๗. **“ความเสี่ยง” (Risk)** หมายถึง โอกาสของสินทรัพย์ของระบบเทคโนโลยีสารสนเทศที่ถูกละเมิดหรือฝ่าฝืนการรักษาความมั่นคงปลอดภัย

๑๘. **“นโยบายการบริหารความเสี่ยงระบบเทคโนโลยีสารสนเทศ” (IT Risk Management Policy)** หมายถึง แนวทางในการบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ ให้สามารถดำเนินการ ประเมินความเสี่ยงได้อย่างมีประสิทธิผลและสอดคล้องกับการประเมินความเสี่ยงของ อ.ต.ก.

๑๙. **“การบริหารความต่อเนื่องทางธุรกิจระบบเทคโนโลยีสารสนเทศ” (Business Continuity for Information Technology)** หมายถึง แนวทางในการบริหารจัดการธุรกิจได้อย่างต่อเนื่องเมื่อ อ.ต.ก. อยู่ ในสภาวะวิกฤติและเหตุฉุกเฉินต่างๆ ทำให้มั่นใจได้ว่า ขั้นตอนการดำเนินงานและระบบสารสนเทศต่างๆ ของ อ.ต.ก. ที่สำคัญได้รับการวางแผนความต่อเนื่องในการดำเนินงานของ อ.ต.ก. (Business Continuity Plan หรือ BCP) อย่างเหมาะสม

ส่วนที่ ๑
การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
(IT Asset Management)

<u>วัตถุประสงค์</u>

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของข้อมูล บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึง และใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

<u>แนวทางปฏิบัติ</u>

๑. หน้าที่ความรับผิดชอบต่อทรัพย์สินขององค์กร

๑.๑ ควบคุมและกำกับให้มีการเก็บบันทึกทะเบียนทรัพย์สิน โดยข้อมูลที่จัดเก็บต้องประกอบด้วยข้อมูลที่จำเป็นในการค้นหาเพื่อการใช้งานในภายหลัง

๑.๒ กำหนดบุคลากรผู้มีหน้าที่ดูแลควบคุมการใช้งานทรัพย์สินสารสนเทศ และผู้มีหน้าที่รับผิดชอบทรัพย์สินสารสนเทศอย่างเหมาะสม

๑.๓ กำหนดกฎระเบียบในการใช้งานทรัพย์สินสารสนเทศไว้อย่างชัดเจน โดยจัดทำเป็นเอกสารและมีการประกาศใช้ในองค์กร

๑.๔ กำหนดให้มีการทบทวนและวางแผนรองรับทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใกล้จะสิ้นสุดตามอายุการใช้งาน (end of life) หรือสิ้นสุดการให้บริการ (end of support) จากผู้ผลิตได้อย่างเหมาะสมทันการณ์

๒. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ

๒.๑ กำหนดให้มีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT inventory list) ของฮาร์ดแวร์ (hardware) และซอฟต์แวร์ (software) ที่รองรับระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. อย่างครบถ้วนและเป็นลายลักษณ์อักษร โดยครอบคลุมอย่างน้อย ดังนี้

- ชื่อเครื่อง
- ชื่อระบบปฏิบัติการ (operating system) และเวอร์ชั่น
- ชื่อระบบงาน (application) และเวอร์ชั่น
- เจ้าของทรัพย์สิน (owner)
- ประเภทของอุปกรณ์ ยี่ห้อ รายละเอียดทางเทคนิค (specification)
- หมายเลขอ้างอิงของฮาร์ดแวร์ (serial number) และหมายเลขอ้างอิงของซอฟต์แวร์ (software license)
- สถานที่ตั้ง
- วันที่เริ่มติดตั้ง

- ประเภทการครอบครอง (ซื้อหรือเช่า)
- รายละเอียดผู้ให้บริการหรือผู้บำรุงรักษา
- วันที่บำรุงรักษาล่าสุด
- วันสิ้นสุดการใช้งานตามสัญญา (warranty) และวันสิ้นสุดการรับประกันการใช้งาน (support contract)
- วันสิ้นสุดการให้บริการจากผู้ผลิต (end of support)

๒.๒ กำหนดให้มีการปรับปรุงทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศให้เป็นปัจจุบันอย่างต่อเนื่อง โดยมีการตรวจสอบ ทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีอยู่จริงกับทะเบียนรายการอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๒.๓ จัดให้มีการบำรุงรักษาทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มีความพร้อมใช้งานและสามารถรองรับการดำเนินธุรกิจได้อย่างต่อเนื่อง

๒.๔ กรณีการโอน ย้าย ยืม ทรัพย์สินสารสนเทศนั้นจะต้องทำใบแจ้งการโอน ย้าย ยืมครุภัณฑ์เป็นลายลักษณ์อักษรถึง ห.กพ. ก่อนดำเนินการ

๒.๕ กำหนดให้มีกระบวนการในการยกเลิกและเรียกคืนทรัพย์สิน (return asset) เมื่อสิ้นสุดการใช้งานครอบคลุมทั้งทรัพย์สินด้านเทคโนโลยีสารสนเทศที่ใช้งานภายใน อ.ต.ก. และกรณีที่ผู้ให้บริการภายนอกมีการใช้งานทรัพย์สินของ อ.ต.ก. ทันทีที่มีการยกเลิกสัญญาจ้างด้วย

๓. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๓.๑ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๓.๑.๑ เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ผู้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร

๓.๑.๒ โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือ แก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมายขององค์กร

๓.๑.๓ ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคล

๓.๑.๔ การตั้งชื่อเครื่องคอมพิวเตอร์ส่วนบุคคล (Computer Name) จะต้องกำหนดโดยเจ้าหน้าที่กองเทคโนโลยีและสารสนเทศ

๓.๑.๕ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ควรมีการตรวจสอบโดยใช้โปรแกรมป้องกันไวรัส

๓.๑.๖ ไม่เก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

๓.๑.๗ ไม่สร้าง Short-cut หรือปุ่มที่สามารถเชื่อมต่อไปยังข้อมูลสำคัญขององค์กร

๓.๑.๘ ผู้ใช้มีหน้าที่รับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยปฏิบัติ ดังนี้

๓.๑.๘.๑ ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

๓.๑.๘.๒ ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

๓.๒ การควบคุมการเข้าถึงระบบปฏิบัติการคอมพิวเตอร์

๓.๒.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่าน ในการเข้าใช้งานระบบปฏิบัติการ

๓.๒.๒ ผู้ใช้ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน และรหัสผ่าน ของตนร่วมกันในการเข้าใช้เครื่อง

๓.๒.๓ ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้ควร Logout ออกจากเครื่องคอมพิวเตอร์หรือ ล็อคหน้าจอด้วยโปรแกรมพักหน้าจอ Screen Saver เมื่อไม่มีการใช้งานโดยตั้งเวลาประมาณ ๑๐ นาที

๓.๒.๔ มีการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศ เมื่อไม่มีการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

๓.๓ การสำรองข้อมูลและการกู้คืนเครื่องคอมพิวเตอร์

๓.๓.๑ ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk และ Flashdrive เป็นต้น

๓.๓.๒ ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง ไว้ในสถานที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลสำรองอย่างสม่ำเสมอ

๓.๓.๓ ผู้ใช้ควรประเมินความเสี่ยงว่า ข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสีย ก็จะไม่กระทบต่อการดำเนินงานขององค์กร

๔. การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๔.๑ การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๔.๑.๑ เครื่องคอมพิวเตอร์แบบพกพาที่องค์กรอนุญาตให้ผู้ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้น ผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานขององค์กร

๔.๑.๒ โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กร ต้องเป็นโปรแกรมที่องค์กรได้ซื้อ ลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่อง คอมพิวเตอร์ส่วนตัว หรือ แก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๔.๑.๓ การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่กองเทคโนโลยีและสารสนเทศ

๔.๑.๔ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๔.๑.๕ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

๔.๑..๖ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๔.๑.๗ หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๔.๑.๘ ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๔.๑.๙ ไม่เคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

๔.๑.๑๐ ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่างๆ เป็นต้น

๔.๑.๑๑ ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า ๓๕ องศาเซลเซียส

๔.๒. การป้องกันความปลอดภัยทางด้านกายภาพ

๔.๒.๑ ผู้ใช้มีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๔.๒.๒ ผู้ใช้ไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

๔.๒.๓ ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่

๔.๓ การควบคุมการเข้าถึงระบบปฏิบัติการ

๔.๓.๑ ผู้ใช้ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งาน ระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

๔.๓.๒ ผู้ใช้ควรตั้งการใช้งานโปรแกรมพักหน้าจอ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งานหลังจากนั้น เมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

๔.๓.๓ ผู้ใช้ต้องทำการ Logout ออกจากระบบทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๔.๔ การสำรองข้อมูลและการกู้คืนเครื่องคอมพิวเตอร์แบบพกพา

๔.๔.๑ ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk และ Flashdrive เป็นต้น

๔.๔.๒ ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง ไว้ในสถานที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของ ข้อมูลและทดสอบการกู้คืนข้อมูลสำรองไว้อย่างสม่ำเสมอ

๔.๔.๓ ผู้ใช้ควรประเมินความเสี่ยงว่า ข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสีย ก็จะไม่กระทบต่อการดำเนินงานขององค์กร

ส่วนที่ ๒
การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ
(Data and Information Security)

วัตถุประสงค์

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการรักษาความมั่นคงปลอดภัยด้านของข้อมูลสารสนเทศ (Data and Information Security) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของข้อมูล บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึง และใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

แนวทางปฏิบัติ

๑. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๑.๑ ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล กำหนดบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน (Password) วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงการใช้งานสารสนเทศในแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบเทคโนโลยีสารสนเทศ รวมถึงวิธีการทำลายข้อมูลในแต่ละประเภทชั้นความลับ

๑.๒ เจ้าของข้อมูล (Information Owner) ต้องทบทวนความเหมาะสมของสิทธิ์ในการเข้าถึงการใช้งานระบบสารสนเทศของผู้ใช้งานเหล่านี้ อย่างน้อยปีละ ๑ ครั้ง

๑.๓ การรับส่งข้อมูลสำคัญผ่านเครือข่ายอินเตอร์เน็ท (Internet) ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากลได้แก่ SSL, VPN หรือ XML Encryption

๒. การแลกเปลี่ยนข้อมูลสารสนเทศ

๒.๑ ต้องกำหนดให้มีนโยบายและขั้นตอนปฏิบัติงานสำหรับการแลกเปลี่ยนข้อมูลสารสนเทศระหว่างหน่วยงานภายในองค์กร และระหว่างองค์กรกับหน่วยงานภายนอก รวมทั้งควบคุมการแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารในรูปแบบข้อมูลอิเล็กทรอนิกส์

๒.๒ การแลกเปลี่ยนข้อมูลสารสนเทศผ่านช่องทางการสื่อสารทุกชนิดระหว่าง อ.ต.ก. กับหน่วยงานภายนอกต้องได้รับการอนุมัติจากผู้บริหารของ อ.ต.ก.

๒.๓ ต้องควบคุมให้มีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูลสารสนเทศหรือซอฟต์แวร์ระหว่างหน่วยงานกับบุคคลหรือหน่วยงานภายนอก

๒.๔ ข้อตกลงการแลกเปลี่ยนข้อมูลสารสนเทศต้องดำเนินการจัดทำอย่างเป็นลายลักษณ์อักษร

๒.๕ การแลกเปลี่ยนข้อมูลสารสนเทศระหว่าง อ.ต.ก. กับหน่วยงานภายนอกต้องดำเนินการแลกเปลี่ยนข้อมูลสารสนเทศด้วยวิธีการที่มีความมั่นคงปลอดภัยและสอดคล้องกับการจัดระดับชั้นสารสนเทศ

๒.๖ ผู้ดูแลระบบ ต้องป้องกันข้อมูลสารสนเทศที่มีการสื่อสารหรือแลกเปลี่ยนในการทำธุรกรรมทางออนไลน์ (Online Transaction) เพื่อมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่ หรือมีการรั่วไหลของข้อมูลหรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ หรือถูกส่งซ้ำโดยมิได้รับอนุญาต

๒.๗ ผู้ดูแลระบบ ต้องมีการป้องกันข้อมูลสารสนเทศที่มีการสื่อสารกันผ่านข้อมูลอิเล็กทรอนิกส์ (Electronic Messaging) เช่น จดหมายอิเล็กทรอนิกส์ (E-mail)

๓. การควบคุมการโอนย้ายข้อมูล (Data Migration)

๓.๑ การโอนย้ายข้อมูล (Data Migration) ต้องกำหนดขั้นตอนการปฏิบัติอย่างชัดเจนด้วยวิธีการที่มีความมั่นคงปลอดภัย ทั้งนี้ เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศยังคงมีความครบถ้วนถูกต้อง และพร้อมใช้งานอยู่เสมอ

ส่วนที่ ๓
การควบคุมการเข้าถึง
(Access Control)

<u>วัตถุประสงค์</u>

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของข้อมูล บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึง และใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

๓. เพื่อให้มีการตรวจสอบและติดตามการพิสูจน์ตัวบุคคลที่เข้าถึงและใช้งานสารสนเทศของ อ.ต.ก. ได้อย่างถูกต้อง

<u>แนวทางปฏิบัติ</u>

๑. การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control)

๑.๑ ผู้ดูแลระบบต้องจำแนกกลุ่มทรัพยากร ได้แก่ ข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ โดยกำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

๑.๒ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงและการใช้งานสารสนเทศให้เหมาะสมตามสิทธิ์และหน้าที่ความรับผิดชอบ ในการปฏิบัติงานของผู้ใช้งานรวมทั้งการทบทวนสิทธิ์อย่างสม่ำเสมอ ดังนี้

๑.๒.๑ กำหนดเกณฑ์ในการอนุญาตในการเข้าถึงและการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้เหมาะสมกับการใช้งาน ดังนี้

๑.๒.๑.๑ สิทธิ์ในการสร้างสารสนเทศ

๑.๒.๑.๒ สิทธิ์ในการอ่านหรือเรียกดูสารสนเทศ

๑.๒.๑.๓ สิทธิ์ในการปรับปรุงหรือเปลี่ยนแปลงสารสนเทศ

๑.๒.๑.๔ สิทธิ์ในการรับรองการปรับปรุงหรือเปลี่ยนแปลงสารสนเทศ

๑.๒.๑.๕ สิทธิ์ในการรับรองความครบถ้วนและถูกต้องของสารสนเทศ

๑.๒.๑.๖ สิทธิ์ในการมอบอำนาจหรือดำเนินการแทน

๑.๒.๑.๗ ไม่มีสิทธิ์

๑.๒.๒ กำหนดเกณฑ์ในการระงับสิทธิ์ มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑.๓ การจัดแบ่งประเภทสารสนเทศ การกำหนดลำดับความสำคัญหรือระดับชั้นความลับของสารสนเทศ การกำหนดระดับชั้นในการเข้าถึงสารสนเทศ การกำหนดช่วงเวลาและช่องทางในการเข้าถึงและการใช้งานสารสนเทศ ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

๑.๓.๑ การจัดแบ่งประเภทของสารสนเทศ

๑.๓.๑.๑ สารสนเทศด้านยุทธศาสตร์

๑.๓.๑.๒ สารสนเทศด้านบัญชี การเงิน งบประมาณ

๑.๓.๑.๓ สารสนเทศด้านบุคลากร

๑.๓.๑.๔ สารสนเทศด้านระบบเทคโนโลยีสารสนเทศ

๑.๓.๑.๕ สารสนเทศด้านการตลาด ธุรกิจ

๑.๓.๑.๖ สารสนเทศเอกสารและสื่อเผยแพร่

๑.๓.๑.๗ สารสนเทศส่วนบุคคล

๑.๓.๒ การกำหนดลำดับความสำคัญหรือระดับชั้นความลับของสารสนเทศ

๑.๓.๒.๑ สารสนเทศลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๑.๓.๒.๒ สารสนเทศลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๑.๓.๓ การกำหนดระดับชั้นในการเข้าถึงสารสนเทศ

๑.๓.๓.๑ ระดับชั้นสำหรับผู้บริหารระดับสูงสามารถเข้าถึงสารสนเทศด้านการบริหาร การตัดสินใจ การจัดการและปฏิบัติงานทุกประเภท

๑.๓.๓.๒ ระดับชั้นสำหรับผู้บริหารสามารถเข้าถึงสารสนเทศทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๑.๓.๓.๓ ระดับชั้นสำหรับผู้ใช้งานสามารถเข้าถึงสารสนเทศด้านการปฏิบัติงาน

๑.๓.๓.๔ ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมายสามารถเข้าถึงสารสนเทศได้ทุกประเภทตามที่ได้รับมอบหมาย

๑.๓.๔ การกำหนดช่องทางในการเข้าถึงและการใช้งานข้อมูล

๑.๓.๔.๑ ติดต่อด้วยตนเอง (ในเวลาทำการ)

๑.๓.๔.๒ โทรศัพท์หรือโทรสาร (ในเวลาทำการ)

๑.๓.๔.๓ เอกสารหรือบันทึกข้อความ (ในเวลาทำการ)

๑.๓.๔.๔ ระบบอินทราเน็ท (ตลอดเวลา)

๑.๓.๔.๕ ระบบอินเตอร์เน็ท (ตลอดเวลา)

๑.๓.๔.๖ ระบบจดหมายอิเล็กทรอนิกส์ (ตลอดเวลา)

๑.๓.๔.๗ เว็บไซต์ (ตลอดเวลา)

๑.๓.๔.๘ การประชุมทางไกล (กรณีเร่งด่วน)

๑.๔ จัดทำป้ายชื่อข้อมูลสารสนเทศ ให้สอดคล้องตามระดับชั้นความลับของสารสนเทศตามที่ อ.ต.ก. กำหนด เพื่อให้แน่ใจว่ามีการแบ่งระดับชั้นข้อมูลที่ถูกต้องและนำไปใช้อย่างเหมาะสม

๑.๕ ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการเข้าถึงและการใช้งานสารสนเทศของ อ.ต.ก. และตรวจสอบการละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๖ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดของการเข้าถึงและการใช้งานสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ

๑.๗ ผู้ดูแลระบบต้องจัดให้มีการบันทึกการผ่านเข้า-ออกพื้นที่ติดตั้งระบบเทคโนโลยีสารสนเทศ

๑.๘ ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Business Requirements for Access Control)

๑.๘.๑ การกำหนดแนวทางการควบคุมการเข้าถึงและการใช้งานสารสนเทศและสิทธิ์ที่เกี่ยวข้องกับสารสนเทศ

๑.๘.๒ การปรับปรุงการควบคุมการเข้าถึงและการใช้งานสารสนเทศให้สอดคล้องกับข้อกำหนดของการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัยด้านสารสนเทศ

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑ ขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User Registration)

<u>สำหรับผู้ดูแลระบบ (System Administrator)</u>

๒.๑.๑ จัดทำแบบฟอร์มขอใช้ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย เพื่อตรวจสอบสิทธิ์และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน (User Registration)

๒.๑.๒ ระบุบัญชีรายชื่อผู้ใช้งานแยกกันเป็นรายบุคคล เพื่อไม่ให้เกิดความซ้ำซ้อนกัน

๒.๑.๓ กำหนดบัญชีรายชื่อผู้ใช้งานโดยกำหนดจากชื่อภาษาอังกฤษคั่นด้วยเครื่องหมายมหัพภาค (.) และตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สองหรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

๒.๑.๔ จำกัดการใช้งานบัญชีรายชื่อผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกันและอนุญาตให้ใช้ระบบเทคโนโลยีสารสนเทศเท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น

๒.๑.๕ ตรวจสอบและมอบหมายสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศที่เหมาะสมต่อหน้าที่และความรับผิดชอบของผู้ใช้งาน

๒.๑.๖ จัดทำเอกสารแสดงถึงสิทธิ์ หน้าที่ และความรับผิดชอบของผู้ใช้งานโดยผู้ใช้งานต้องลงนามรับทราบ

๒.๑.๗ บันทึกและจัดเก็บข้อมูลการขออนุมัติการเข้าใช้ระบบเทคโนโลยีสารสนเทศ

<u>สำหรับผู้ใช้งาน (User)</u>

๒.๑.๘ ผู้ใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตก่อนจึงจะมีสิทธิ์เข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศของ อ.ต.ก.

๒.๑.๙ ผู้ดูแลระบบกำหนดหรือทบทวนหลักเกณฑ์ในการยกเลิกหรือเพิกถอนการอนุญาตและการระงับการใช้สิทธิ์ในการข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. จากบัญชีรายชื่อผู้ใช้งานเมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการเป็นพนักงาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ดังนี้

๒.๑.๙.๑ บรรจุพนักงานใหม่ ภายใน ๗ วันทำการ

๒.๑.๙.๒ เปลี่ยนแปลง/โอนย้าย/แต่งตั้ง/ปรับระดับ ภายใน ๗ วันทำการ

๒.๑.๙.๓ ลาออก ภายใน ๗ วันทำการ

๒.๒ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ์ เพื่อให้ผู้ใช้งานสามารถเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศแต่ละระบบตามการปฏิบัติหน้าที่ รวมถึงสิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๒.๒.๑ ผู้ดูแลระบบกำหนดการมอบหมายหรือกำหนดสิทธิ์การใช้งานให้แก่ผู้ใช้งาน

๒.๒.๒ ผู้ดูแลระบบกำหนดระดับของสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบและตามความจำเป็นในการใช้งาน

๒.๒.๓ ผู้ดูแลระบบต้องมอบหมายสิทธิ์ที่สอดคล้องกับนโยบายควบคุมการเข้าถึง

๒.๒.๔ ผู้ดูแลระบบบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน

๒.๒.๕ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ก่อนการดำเนินการ โดยกำหนดระยะเวลาการใช้งานและระงับการใช้งานระบบเทคโนโลยีสารสนเทศตามเกณฑ์การกำหนดสิทธิ์

๒.๓ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) จัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

๒.๓.๑ การกำหนดรายชื่อผู้ใช้งานต้องไม่ซ้ำกัน

๒.๓.๒ การเปลี่ยนแปลงและยกเลิกรหัสผ่าน เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

๒.๓.๓ การตั้งรหัสผ่านชั่วคราวต้องยากต่อการคาดเดาและต้องมีความแตกต่างกันและความหลากลายของอักขระ

๒.๓.๔ การส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานต้องส่งมอบด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือผ่านทางซอฟต์แวร์ต่าง ๆ ในการจัดส่งรหัสผ่านซึ่งผู้ใช้งานควรตอบกลับทันทีหลังจากได้รับรหัสผ่านเรียบร้อยแล้ว

๒.๓.๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราวและควรเปลี่ยนให้รหัสผ่านยากต่อการเดาและต้องมีความแตกต่างกันและหลากลายของอักขระ ซึ่งประกอบด้วย ตัวอักษร ตัวเลข หรือสัญลักษณ์อื่นใดที่ยากต่อการคาดเดา

๒.๓.๖ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากที่ผู้ดูแลระบบติดตั้งซอฟต์แวร์แล้วเสร็จ

๒.๓.๗ ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ในรูปแบบข้อความหรือไฟล์ที่ไม่ได้ป้องกันการเข้าถึง

๒.๓.๘ การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีรายชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่อนุญาตให้เปลี่ยนรหัสใหม่

๒.๓.๙ ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นต้องได้รับความเห็นชอบและอนุมัติจาก ห.กส. ก่อนการดำเนินการ โดยกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และต้องกำหนดสิทธิ์พิเศษที่ได้รับว่าสามารถเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๔ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบเทคโนโลยีสารสนเทศและปรับปรุงบัญชีรายชื่อผู้ใช้งาน ดังนี้

๒.๔.๑ สิทธิ์การเข้าถึงข้อมูลของผู้ใช้งาน (User Access Rights) ได้รับการพิจารณาทบทวนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดทุก ๆ ๖ เดือน หรือเมื่อการเปลี่ยนแปลง ดังนี้

๒.๔.๑.๑ การบรรจุพนักงานใหม่ ภายใน ๗ วัน

๒.๔.๑.๒ เมื่อมีคำสั่งเปลี่ยนแปลง/โอนย้าย/แต่งตั้งปรับระดับพนักงาน ภายใน ๗ วัน

๒.๔.๑.๓ การลาออกของพนักงาน ภายใน ๗ วัน

๒.๔.๒ การให้อำนาจสำหรับสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งานพิเศษต้องมีการทบทวนที่มีความถี่มากกว่าโดยทบทวนอย่างน้อยทุก ๆ ๓ เดือน

๒.๔.๓ การจัดสรรสิทธิ์พิเศษต้องได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดเพื่อให้มั่นใจได้ว่าไม่มีการให้สิทธิ์พิเศษกับผู้ใช้งานที่ไม่ได้รับมอบอำนาจ

๒.๔.๔ ความเปลี่ยนแปลงของผู้ใช้งานที่ได้รับสิทธิ์พิเศษต้องถูกบันทึกเพื่อการทบทวน

๓. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๓.๑ การกำหนดขั้นตอนการเข้าถึงระบบปฏิบัติการ ดังนี้

๓.๑.๑ กส. ต้องกำกับให้มีการควบคุมในการเข้าถึงระบบปฏิบัติการอย่างมั่นคง ปลอดภัย โดยขั้นตอนการเข้าสู่ระบบ ต้องมีการเปิดเผยข้อมูลเกี่ยวกับระบบให้น้อยที่สุดเพื่อหลีกเลี่ยงผู้ใช้งาน ที่ไม่ได้รับอนุญาต

๓.๑.๒ ต้องกำหนดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน (Password)

๓.๑.๓ ต้องกำหนดให้ระบบแสดงข้อความเตือน “อนุญาตเฉพาะบุคคลที่เกี่ยวข้องมีสิทธิ์เข้าใช้งานเท่านั้น”

๓.๑.๔ จำกัดการเชื่อมต่อผ่าน Command Line

๓.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๓.๒.๑ ต้องกำหนดให้มีบัญชีรายชื่อผู้ใช้งานของแต่ละบุคคลเพื่อใช้ในการพิสูจน์ตัวตน

๓.๒.๒ ผู้ใช้งานทุกคนต้องผ่านระบบพิสูจน์ตัวตนก่อนเข้าใช้งานระบบปฏิบัติการ โดยแสดงชื่อบัญชีผู้ใช้งานและรหัสผ่าน (Password) และเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราวต้องทำการออกจากระบบ (Logout) ทุกครั้ง

๓.๓ การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำมาตรการและการกำหนดรหัสผ่านตามมาตรฐานสากลที่พึงปฏิบัติ พร้อมจัดหลักสูตรอบรมการสร้างความตระหนักให้กับผู้ใช้งาน ดังนี้

๓.๓.๑ ผู้ใช้งาน ต้องกำหนดรหัสผ่านให้มีความมั่นคงปลอดภัย โดยรหัสผ่านจะต้องประกอบด้วย

๑) ความยาวไม่น้อยกว่า ๘ ตัวอักขระ

๒) การตั้งรหัสผ่านจะต้องประกอบไปด้วยอักขระอย่างน้อย ๔ ประเภท ดังนี้

- ตัวเลข (Numerical Character)
- ตัวอักษร (Alphabet) พิมพ์ใหญ่
- ตัวอักษร (Alphabet) พิมพ์เล็ก
- ตัวอักขระพิเศษ (Special Character)

๓.๓.๒ ผู้ใช้งานต้องไม่ตั้งรหัสผ่านด้วย ชื่อ วันเดือนปีเกิด หรือข้อความใดที่ง่ายต่อการล่วงรู้หรือง่ายต่อการคาดเดา

๓.๓.๓ ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว อย่างน้อย ๓ รหัสผ่านที่เคยใช้งานล่าสุด

๓.๓.๔ ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่าน ทุก ๆ ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๓.๓.๕ ผู้ดูแลระบบจะต้องควบคุมให้ระบบตัดการเชื่อมต่อ หากมีการยืนยันตัวตนไม่ถูกต้องติดต่อกันมากกว่า ๓ ครั้ง

๓.๓.๖ ผู้ใช้งานต้องใช้งานรหัสผ่านอย่างระมัดระวัง ไม่เปิดเผยรหัสผ่านให้ผู้อื่นได้รับรู้และต้องรับผิดชอบหากเกิดความเสียหายจากการนำรหัสผ่านไปใช้ในทุกกรณี

๓.๓.๗ ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง และต้องไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น

๓.๓.๘ ผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านครั้งแรกทันที หลังจากที่ได้รับชื่อการเข้าใช้งานและรหัสผ่าน

๓.๔ การใช้งานซอฟต์แวร์อรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานซอฟต์แวร์อรรถประโยชน์สำหรับเครื่องคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานซอฟต์แวร์บางชนิดสามารถทำให้ผู้ใช้งานละเมิดหรือฝ่าฝืนมาตรการป้องกันด้านความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศได้ เพื่อป้องกันการกระทำดังกล่าวให้ดำเนินการดังนี้

๓.๔.๑ จำกัดสิทธิ์การเข้าถึงและกำหนดสิทธิ์ผู้ใช้งานอย่างรัดกุมในการอนุญาตให้ใช้ซอฟต์แวร์ช่วยเหลือต่างๆ

๓.๔.๒ อนุญาตให้ใช้งานซอฟต์แวร์ที่ อ.ต.ก. จัดหาให้และต้องมีลิขสิทธิ์เท่านั้น

๓.๔.๓ ห้ามติดตั้งซอฟต์แวร์ใดๆ โดยไม่ได้รับอนุญาต

๓.๔.๔ ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องควบคุมให้มีการจำกัดการเข้าถึงซอร์สโค้ด (Source Code) ของโปรแกรม

๓.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบเทคโนโลยีสารสนเทศนั้น (Session time-out)

โดยผู้ดูแลระบบต้องตัดเวลาการใช้งานของเครื่องคอมพิวเตอร์เมื่อผู้ใช้งานไม่ได้ใช้งานเป็นระยะเวลาเกิน ๑๕ นาที (Session Timeout)

๔. การควบคุมการเข้าถึงซอฟต์แวร์ประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุมอย่างน้อยดังนี้

๔.๑ การควบคุมการเข้าถึงซอฟต์แวร์ประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Information Access Restriction)

๔.๑.๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานใหม่ปฏิบัติ ดังนี้

๔.๑.๑.๑ การลงทะเบียนผู้ใช้งาน (User Registration)

๔.๑.๑.๒ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (Privilege Management)

๔.๑.๑.๓ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๔.๑.๑.๔ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Right)

๔.๑.๒ การเข้าถึงแอปพลิเคชั่นผ่านทางเครือข่ายของ อ.ต.ก. ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนผู้ใช้งานที่ปลอดภัย โดยใช้บัญชีรายชื่อผู้ใช้งานและรหัสผ่าน

๔.๑.๓ การเข้าถึงแอปพลิเคชั่นผ่านทางเครือข่ายอินเตอร์เน็ทให้ใช้ช่องทาง Secure Sockets Layer Virtual Private Network (SSL VPN) และต้องกำหนดให้มีการพิสูจน์ตัวตนผู้ใช้งานที่ปลอดภัย โดยใช้บัญชีรายชื่อผู้ใช้ (User Account) และรหัสผ่าน (Password)

๔.๑.๕ ผู้ดูแลระบบ (System Administrator) ต้องบันทึกข้อมูลหรือพฤติกรรมการใช้งานข้อมูล โดยจัดเก็บ Audit Log เป็น Log File ที่ใช้เก็บข้อมูลการเข้าถึงระบบของผู้ใช้งานเพื่อตรวจสอบว่าใครนำเข้ามาใช้งานในระบบการตรวจสอบการบุกรุก

๔.๑.๖ ในกรณีมีการจ้างพนักงาน Outsource กำหนดมาตรการในการควบคุมการเข้าถึงแอปพลิเคชั่นและสารสนเทศ ดังนี้

๔.๑.๖.๑ กำหนดให้มีเจ้าหน้าที่ผู้ควบคุมงานกำกับดูแลการดำเนินงานต่าง ๆ ของพนักงาน Outsource

๔.๑.๖.๒ แจ้งให้พนักงาน Outsource รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ อ.ต.ก.

๔.๑.๖.๓ กำหนดให้พนักงาน Outsource ลงนามในแบบฟอร์มการรักษาความลับของข้อมูล

๔.๒ กำหนดคุณสมบัติการการเข้าถึงแอปพลิเคชั่นและสารสนเทศ ดังนี้

๔.๒.๑ ไม่มีหรือไม่แสดง Function ให้ความช่วยเหลือระหว่างการล๊อคอิน (Login)

๔.๒.๒ บันทึกความพยายามในการล๊อคอิน (Login) ที่สำเร็จและไม่สำเร็จ และแสดงประวัติการล๊อคอิน (Login) ๓ ครั้งล่าสุด

๔.๒.๓ ตัดการเชื่อมต่อหลังจากการล๊อคอิน (Login) ไม่สำเร็จเกินกว่า ๓ ครั้ง

๔.๓ การแยกระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูง

๔.๓.๑ ระบบเทคโนโลยีสารสนเทศมีความสำคัญต่อ อ.ต.ก. สูงต้องถูกแยกออกจากระบบเทคโนโลยีสารสนเทศอื่นๆ ได้แก่ ระบบเทคโนโลยีสารสนเทศด้านการบัญชีการเงิน เว็บไซต์ของ อ.ต.ก. ระบบจดหมายอิเล็กทรอนิกส์ และระบบศูนย์ปฏิบัติการ (Operation Center)

๔.๓.๒ ต้องจัดทำระบบสำรองของระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูงตามแนวปฏิบัติที่เกี่ยวข้องกับการสำรองข้อมูลและระบบเทคโนโลยีสารสนเทศ และการเตรียมความพร้อมกรณีฉุกเฉินตามที่ อ.ต.ก. กำหนด

๔.๓.๓ ต้องมีเครื่องมือ (Tools) เพื่อใช้ในการตรวจสอบสภาพพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูง ได้แก่ ระบบ Network Monitoring และระบบ Application Monitoring

๔.๔ การปฏิบัติงานจากภายนอก อ.ต.ก. (Teleworking)

๔.๔.๑ กำหนดการเข้าถึงแอปพลิเคชั่นและสารสนเทศได้ ๒ ช่องทาง ดังนี้

๔.๔.๑.๑ การเข้าถึงแอปพลิเคชั่นและสารสนเทศที่เปิดให้ใช้งานจากภายนอกได้โดยตรง ได้แก่ เว็บไซต์ของ อ.ต.ก., ระบบ E-mail

๔.๔.๑.๒ การเข้าถึงแอปพลิเคชั่นและสารสนเทศผ่าน SSL-VPN ของ อ.ต.ก.

๔.๔.๒ ตรวจสอบอุปกรณ์ที่เป็นของส่วนตัวที่ใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. จากระยะไกลต้องมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่ อ.ต.ก. กำหนด

๔.๔.๓ ผู้ใช้งานที่ทำการเข้าถึงระบบเครือข่ายจากระยะไกลทุกคนต้องผ่านการพิสูจน์ตัวตนเพื่อเพิ่มความปลอดภัยและต้องมีการตรวจสอบ ได้แก่ รหัสผ่าน (Password) หรือวิธีการเข้ารหัส (Encryption)

๔.๔.๔ ไม่อนุญาตให้ใช้งานอุปกรณ์ฮาร์ดแวร์ที่เป็นของส่วนตัว เพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศจากระยะไกลหากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคง ปลอดภัยสารสนเทศของ อ.ต.ก.

๔.๔.๕ ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของสารสนเทศ ระบบงานและบริการต่าง ๆ ของ อ.ต.ก. ที่อนุญาตและไม่อนุญาตให้มีการเข้าถึงระบบเครือข่ายจากระยะไกล

๔.๔.๖ ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบเครือข่ายจากระยะไกล

๕. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๕.๑ กำหนดมาตรการควบคุมการเข้าถึงและการใช้งานคอมพิวเตอร์แม่ข่าย (Server) ดังนี้

๕.๑.๑ บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าถึงคอมพิวเตอร์แม่ข่ายของ อ.ต.ก. ต้องขออนุญาตเป็นลายลักษณ์อักษร และต้องได้รับอนุญาตจาก ห.กส. ก่อนดำเนินการ

๕.๑.๒ ผู้ดูแลระบบต้องไม่เปิดพอร์ตที่ใช้ทิ้งเอาไว้โดยไม่จำเป็นและพอร์ตดังกล่าวต้องตัดการเชื่อมต่อ เมื่อไม่ได้ใช้งานแล้วโดยอัตโนมัติและเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๕.๑.๓ วิธีการใดๆ ที่สามารถเข้าถึงระบบเครือข่ายจากระยะไกลได้ จำเป็นต้องได้รับการอนุญาตจาก ห.กส. ก่อนการดำเนินการ

๕.๑.๔ กำหนดให้การเข้าถึงคอมพิวเตอร์แม่ข่าย (Server) ต้องใช้มาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าถึงระบบเทคโนโลยีสารสนเทศภายใน เช่น VPN หรือ SSL เป็นต้น

๕.๒ การติดตั้งซอฟต์แวร์บนเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๕.๒.๑ ห้ามผู้ที่ไม่ได้รับอนุญาตเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือกระทำการใดๆ ต่ออุปกรณ์ของเครื่องแม่ข่าย อุปกรณ์ต่อพ่วง หรืออุปกรณ์ฮาร์ดแวร์อื่นๆ ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) หรืออุปกรณ์อื่น ๆ ที่เกี่ยวข้อง โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

๕.๒.๒ ผู้ดูแลระบบต้องบริหารควบคุมคอมพิวเตอร์แม่ข่ายและรับผิดชอบ

๕.๓ ทบทวนการทำงานของระบบเทคโนโลยีสารสนเทศหลังจากที่มีการเปลี่ยนแปลงระบบ

๕.๓.๑ แจ้งให้ผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงของระบบเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบ

๕.๓.๒ พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศรวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในกรณีที่ อ.ต.ก. ต้องเปลี่ยนไปใช้ระบบเทคโนโลยีสารสนเทศใหม่

๕.๔ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๕.๔.๑ ผู้พัฒนาระบบภายนอกต้องปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ อ.ต.ก. อย่างเคร่งครัด

๕.๔.๒ จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์สำหรับผู้รับจ้างจากภายนอก

๕.๔.๓ ระบุว่าใครเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาซอร์สโค้ดในการพัฒนาซอฟต์แวร์

๕.๔.๔ กำหนดเรื่องการสงวนสิทธิ์เพื่อตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่มีการพัฒนา โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้รับจ้างจากภายนอกนั้น

๕.๕ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลงการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังนี้

๕.๕.๑ เก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้

๕.๕.๒ กำหนดให้มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บและกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าวเพื่อรักษาความน่าเชื่อถือของข้อมูลและไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้เว้นแต่ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้เช่นผู้ตรวจสอบภายในด้านระบบเทคโนโลยีสารสนเทศ (Internal IT Auditor) หรือผู้ตรวจสอบอิสระภายนอก (External IT Auditor) ที่ อ.ต.ก. มอบหมาย

๕.๕.๓ การเก็บข้อมูลจราจรต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

๕.๕.๔ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งเวลาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล

๖. การควบคุมการเข้าใช้งานระบบจากภายนอก

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กรเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกโดยมีแนวทางปฏิบัติดังนี้

๖.๑ การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กรก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรขององค์กรการควบคุมบุคคลที่เข้าสู่ระบบขององค์กรจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๖.๒ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุมัติจาก ห.กส. ก่อนและมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๖.๓ ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกลผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๖.๔ ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๖.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่ควรเปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็นช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

ส่วนที่ ๔
การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
(Physical and Environmental Security)

วัตถุประสงค์

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and Environmental Security) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของสารสนเทศ บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้ เข้าถึงและใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

แนวทางปฏิบัติ

๑. การรักษาความมั่นคงปลอดภัยด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๑.๑ การกำหนดบริเวณหรือพื้นที่

๑.๑.๑ กำหนดพื้นที่การใช้งานระบบเทคโนโลยีสารสนเทศที่ต้องมีการรักษาความมั่นคงปลอดภัย

๑.๑.๒ กำหนดการควบคุมการเข้า-ออกพื้นที่ติดตั้งระบบเทคโนโลยีสารสนเทศ

๑.๑.๓ บุคคลภายนอกหรือหน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์ที่ใช้ในการปฏิบัติงานและเชื่อมต่อเข้ากับระบบเครือข่ายของ อ.ต.ก. ต้องได้รับอนุญาตจาก ห.กส. หรือ ผู้ดูแลระบบที่ได้รับมอบหมายก่อนการใช้งาน

๑.๑.๔ ควบคุมการเข้าออกพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure Area) ได้แก่ ศูนย์คอมพิวเตอร์ และห้องปฏิบัติงานของเจ้าหน้าที่ศูนย์คอมพิวเตอร์ โดยต้องกำหนดให้เฉพาะผู้มีสิทธิที่สามารถเข้าออกได้ และมีการเก็บบันทึกการเข้าออกศูนย์คอมพิวเตอร์ และบันทึกการเข้าออก ดังกล่าวต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่านเข้าออก รวมถึงต้องมีการตรวจสอบบันทึกดังกล่าวอย่างสม่ำเสมอ

๑.๑.๕ ควบคุมให้มีการออกแบบและติดตั้งการป้องกันความมั่นคงปลอดภัยด้านกายภาพเพื่อป้องกันภัยจากภายนอกภัยในระดับหายนะทั้งที่ก่อโดยมนุษย์หรือภัยธรรมชาติ เช่น อัคคีภัย อุทกภัย แผ่นดินไหว ระเบิด การก่อจลาจล เป็นต้น

๑.๑.๖ กำหนดแนวทางปฏิบัติของการป้องกันทางกายภาพสำหรับการทำงานในพื้นที่ ที่ต้องการรักษาความมั่นคงปลอดภัยด้านกายภาพ (Secure Area) ได้แก่ ศูนย์คอมพิวเตอร์ และห้องปฏิบัติงานของเจ้าหน้าที่ศูนย์คอมพิวเตอร์ และกำหนดให้มีการนำแนวทางปฏิบัติไปใช้งาน

๑.๑.๗ ควบคุมบริเวณที่ผู้ไม่มีสิทธิเข้าถึงอาจสามารถเข้าถึงได้ เช่น จุดรับส่งของ เป็นต้น โดยกำหนดพื้นที่การส่งมอบสินค้า และพื้นที่การเตรียมหรือประกอบอุปกรณ์สารสนเทศก่อนนำเข้าศูนย์

คอมพิวเตอร์ โดยต้องควบคุมการเข้าออกเพื่อหลีกเลี่ยงการเข้าถึงระบบสารสนเทศและข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๑.๑.๘ กำหนดให้มีการจัดวางและป้องกันอุปกรณ์สารสนเทศ เพื่อลดความเสี่ยงจากภัยธรรมชาติหรืออันตรายต่างๆ และเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต

๑.๑.๙ ต้องมีการป้องกันอุปกรณ์สารสนเทศ ที่อาจเกิดจากไฟฟ้าขัดข้อง (Power Failure) หรือที่อาจหยุดชะงักจากข้อผิดพลาดของโครงสร้างพื้นฐาน (Supporting Utilities) โดยจัดหาติดตั้งและบำรุงรักษาอุปกรณ์หรือระบบสนับสนุนในการรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ เช่น อุปกรณ์ดับเพลิง อุปกรณ์สำรองไฟฟ้า ระบบควบคุมอุณหภูมิและความชื้น ระบบเตือนภัยน้ำรั่ว หรือระบบแจ้งเตือนเมื่ออุปกรณ์สารสนเทศทำงานผิดปกติ เป็นต้น

๑.๒ การเดินสายไฟ สายสัญญาณ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

๑.๒.๑ หลีกเลี่ยงการเดินสายสัญญาณของระบบเครือข่ายที่ต้องผ่านบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๑.๒.๒ การเดินสายสัญญาณต้องร้อยท่อเพื่อป้องกันการดักจับสัญญาณหรือการตัดสายสัญญาณทำให้เกิดความเสียหาย

๑.๒.๓ การเดินสายสัญญาณและสายไฟฟ้าต้องแยกออกจากกันเพื่อป้องกันการแทรกแซงหรือรบกวนของสัญญาณซึ่งกันและกัน

๑.๒.๔ ทำป้ายชื่อ (Label) สำหรับสายสัญญาณบนอุปกรณ์เครือข่ายเพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๑.๒.๕ จัดทำผังสายสัญญาณและอุปกรณ์เครือข่ายให้ครบถ้วนและถูกต้อง

๑.๒.๖ ตรวจสอบสายสัญญาณทั้งหมด เพื่อตรวจหาการติดตั้ง ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี อย่างน้อยปีละ ๑ ครั้ง

๑.๓ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๑.๓.๑ บำรุงรักษาอุปกรณ์ของระบบเทคโนโลยีสารสนเทศตามรอบระยะเวลาที่กำหนด

๑.๓.๒ ปฏิบัติตามคำแนะนำของผู้ผลิตอย่างเคร่งครัด

๑.๓.๓ จัดเก็บบันทึกกิจกรรมการบำรุงรักษาทุกครั้ง

๑.๓.๔ จัดเก็บบันทึกปัญหาและข้อบกพร่องและวิธีแก้ปัญหาทุกครั้งที่พบ

๑.๔ การนำทรัพย์สินของ อ.ต.ก. ออกไปใช้งานนอก อ.ต.ก. (Removal of Property)

๑.๔.๑ ผู้ใช้งานต้องแจ้งนำทรัพย์สินของ อ.ต.ก. ออกไปใช้งานนอก อ.ต.ก. และต้องได้รับการอนุญาตจาก ห.กส. หรือผู้ที่ได้รับมอบหมาย ก่อนดำเนินการ

๑.๔.๒ ผู้ใช้งานต้องทำบันทึกแจ้งการนำพัสดุออกจาก อ.ต.ก. เป็นลายลักษณ์อักษร โดยทำเป็น ๒ ฉบับ ฉบับตัวจริงส่งให้กองพัสดุ ส่วนสำเนาผู้ขอเก็บไว้ และต้องได้รับการอนุญาตจาก ห.กพ. ก่อนดำเนินการนำพัสดุออกจาก อ.ต.ก.

๑.๔.๓ เมื่อนำทรัพย์สินของ อ.ต.ก. ส่งคืน ผู้ดูแลระบบต้องตรวจสอบการชำรุดเสียหายของทรัพย์สินของ อ.ต.ก. ที่นำออกไปใช้ภายนอก อ.ต.ก.

๑.๔.๔ ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของ อ.ต.ก. ไว้โดยลำพังในที่สาธารณะ ผู้ใช้งานต้องรับผิดชอบดูแลเสมือนเป็นทรัพย์สินของตนเอง

๑.๔.๕ ควบคุมให้มีขั้นตอนการปฏิบัติงานสำหรับการบริหารจัดการอุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลอิเล็กทรอนิกส์ที่สามารถถอดหรือต่อพ่วงกับเครื่องคอมพิวเตอร์ได้ (Removable Media)

๑.๔.๖ ต้องมีการป้องกันอุปกรณ์ที่ใช้จัดเก็บข้อมูลสารสนเทศ ในกรณีที่มีการเคลื่อนย้ายอุปกรณ์เพื่อมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือถูกนำไปใช้งานผิดประเภท หรืออุปกรณ์หรือข้อมูลสารสนเทศได้รับความเสียหาย

๑.๕ การป้องกันอุปกรณ์ที่ไม่ใช่ทรัพย์สินของ อ.ต.ก. (Security of Equipment Off-premises)

๑.๕.๑ กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ที่ไม่ใช่ทรัพย์สินของ อ.ต.ก. มาใช้งานใน อ.ต.ก.

๑.๕.๒ ผู้ใช้งานต้องแจ้งการนำทรัพย์สินที่ไม่ใช่ของ อ.ต.ก. เข้ามาใช้งานภายใน อ.ต.ก. โดยผู้ดูแลระบบจะดำเนินการใส่หมายเลข (Mac Address) ของอุปกรณ์นั้นเข้าไปในระบบ เพื่อให้อุปกรณ์นั้นสามารถใช้งานกับระบบเทคโนโลยีสารสนเทศของ อ.ต.ก. ได้

๑.๖ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

๑.๖.๑ กำหนดให้ทำลายสารสนเทศสำคัญก่อนการกำจัดอุปกรณ์หรือหมดสัญญาการใช้งาน

๑.๖.๒ กำหนดมาตรการหรือเทคนิคการลบหรือเขียนทับบนสารสนเทศที่สำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงสารสนเทศที่สำคัญนั้นได้

๑.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารของระบบเทคโนโลยีสารสนเทศ

๑.๗.๑ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๑.๗.๒ กำหนดการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศโดยผู้ที่ได้รับอนุญาตเท่านั้น

๑.๗.๓ ผู้ใช้งานต้องไม่ทิ้งเอกสารที่เป็นลำดับชั้นความลับ ลับมาก ไว้ที่เครื่องถ่ายเอกสาร เครื่องปริ้นท์เตอร์ หรือเครื่องสแกนเนอร์ เมื่อสั่งพิมพ์หรือสำเนาแล้วต้องเก็บเอกสารทันที

๑.๗.๔ ผู้ใช้งานต้องไม่ทิ้งเอกสารสำคัญหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ไว้ที่โต๊ะทำงานโดยไม่มีผู้ดูแล หรือไม่ได้ใช้งาน และต้องจัดหาสถานที่จัดเก็บอย่างปลอดภัย ได้แก่ เก็บในตู้ที่มีอุปกรณ์ล็อค

๒. การควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย

๒.๑ การควบคุมห้องคอมพิวเตอร์แม่ข่ายต้องจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่ายอุปกรณ์เครือข่าย เป็นต้น ไว้ในกองเทคโนโลยีและสารสนเทศหรือพื้นที่หวงห้าม และต้องกำหนดสิทธิการเข้าออก ห้องคอมพิวเตอร์แม่ข่ายให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer operator) เจ้าหน้าที่ดูแลระบบ (system administrator) เป็นต้น ในกรณีบุคคลที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออกห้องคอมพิวเตอร์แม่ข่ายในบางครั้ง ก็ต้อง

มีการควบคุมอย่างรัดกุม เช่น กำหนดให้มีเจ้าหน้าที่กองเทคโนโลยีและสารสนเทศควบคุมดูแลการทำงานตลอดเวลา เป็นต้น ต้องมีระบบเก็บ บันทึกการเข้าออกห้องคอมพิวเตอร์แม่ข่าย โดยการบันทึกต้องมีรายละเอียดเกี่ยวกับตัวบุคคล เวลาผ่าน เข้าออก และสามารถตรวจสอบบันทึกดังกล่าวได้ ห้องคอมพิวเตอร์แม่ข่ายควรจัดให้เป็นสัดส่วน เช่น แบ่งเป็นส่วน ระบบเครือข่าย (network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยัง ทำให้สามารถควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์สำคัญ

๒.๒ ต้องกำหนดให้มีสิทธิให้กับเจ้าหน้าที่ ที่ให้สามารถมีสิทธิในการเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ได้รับมอบหมายประกอบด้วย

๒.๒.๑ จัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

๒.๒.๒ กำหนดผู้มีหน้าที่รับผิดชอบการบันทึกเข้า-ออก ดังกล่าวโดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่

๒.๓ บุคคลภายนอกเข้ามาติดต่อจะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้า - ออก ให้ ถูกต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

๒.๔ บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่ หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

๒.๕ เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการขออนุญาต เข้า-ออก เป็นประจำทุกเดือน

ส่วนที่ ๕
การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร
(Communications Security)

<u>วัตถุประสงค์</u>

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของสารสนเทศ บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้ เข้าถึงและใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

<u>แนวทางปฏิบัติ</u>

๑. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

๑.๑ การใช้บริการของระบบเครือข่าย (Network) ต้องกำหนดให้ผู้ใช้งาน (Users) สามารถเข้าถึงระบบเทคโนโลยีสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๑.๑.๑ ห้ามผู้ใช้งานกระทำการใด ๆ ที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าวย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของ อ.ต.ก.

๑.๑.๒ อ.ต.ก ไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านระบบเครือข่าย เช่น การประกาศแจ้งความการซื้อหรือจำหน่ายสินค้า การนำสารสนเทศไปซื้อขาย การรับบริการค้นหาสารสนเทศโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดปิดบริการอินเทอร์เน็ทแก่บุคคลทั่วไปเพื่อแสวงหากำไร เป็นต้น

๑.๑.๓ ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น กล่าวคือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีรายชื่อผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิ์ของ อ.ต.ก. หรือผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว อ.ต.ก. ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๑.๑.๔ ห้ามมิให้ผู้ใดเข้าใช้งานโดยไม่ได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบเครือข่ายถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของ อ.ต.ก.

๑.๑.๕ การกำหนดบัญชีรายชื่อผู้ใช้งานเป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือแจกจ่ายสิทธิ์นี้ให้กับผู้อื่นไม่ได้

๑.๑.๖ กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๑.๑.๗ ห้ามเปิดหรือใช้งานซอฟต์แวร์ประเภท Peer-to-Peer หรือซอฟต์แวร์ที่มีความเสี่ยงเว้นแต่จะได้รับอนุญาตจาก ห.กส.

๑.๑.๘ การใช้งานอินเตอร์เน็ทจะถูกบันทึกการใช้งานเป็นระยะเวลา ๙๐ วัน ตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๑.๑.๙ ควบคุมให้มีการกำหนดรูปแบบการรักษาความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดการบริหารจัดการในข้อตกลงการให้บริการด้านเครือข่ายคอมพิวเตอร์ ไม่ว่าเป็นการ ให้บริการโดยหน่วยงานเองหรือจ้างช่วงไปยังผู้ให้บริการภายนอก

๑.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอก อ.ต.ก. (User Authentication for External Connections)

๑.๒.๑ การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งานและการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password) หรือวิธีการอื่นที่ อ.ต.ก. กำหนด

๑.๒.๒ การเข้าสู่ระบบจากระยะไกล (Remote Access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งานสิทธิ์ และมีการใช้การเข้ารหัส ได้แก่ VPN

๑.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks)

๑.๓.๑ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ของ อ.ต.ก. โดยมีรายละเอียดของระบบเครือข่ายภายในและระบบเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งดำเนินการปรับปรุงให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

๑.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๑.๔.๑ กำหนดค่าเริ่มต้นพื้นฐานของระบบเครือข่ายต้องเป็นแบบอนุญาตบางส่วนและปฏิเสธทั้งหมด (Permit Any & Deny All)

๑.๔.๒ ผู้ดูแลระบบต้องกำหนดการเปิด–ปิดพอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการการเข้าถึงพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบเครือข่าย

๑.๔.๓ บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใด ๆ ในห้องติดตั้งระบบเครือข่ายหรือระบบเทคโนโลยีสารสนเทศ (Data Center) จะต้องลงชื่อเข้า-ออก ให้ถูกต้องและได้รับการอนุญาตจาก ห.กส. ก่อนเข้าดำเนินการ และจะต้องมีเจ้าหน้าที่ของ อ.ต.ก. อยู่กับบุคคลที่เข้าดำเนินการตลอดเวลา

๑.๔.๔ บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษาบริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่ายต้องได้รับการอนุมัติจาก ห.กส. ก่อนการดำเนินการ

๑.๔.๕ ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๑.๕ การแบ่งแยกเครือข่าย (Segregation in Networks)

๑.๕.๑ ออกแบบระบบเครือข่ายโดยจัดแบ่งตามกลุ่มของระบบเทคโนโลยีสารสนเทศที่มีการใช้งานตามกลุ่มของผู้ใช้งานโดยจัดแบบออกเป็นเขตภายใน (Internal Zone) และเขตภายนอก

(External Zone) และเขตสำหรับการให้บริการ (Demilitarize Zone : DMZ) เพื่อควบคุมและป้องกันการถูกโจมตี

๑.๕.๒ แบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ทางกายภาพตามอาคารและชั้นต่าง ๆ ด้วย วิธีแบ่งแยกเครือข่ายเสมือน (Virtual LAN: VLAN) รวมทั้งให้มีการแบ่งแยกเครือข่ายตามระบบหรือแอปพลิเคชั่นที่มีความสำคัญ

๑.๕.๓ ติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายไว้ในระบบเครือข่ายที่จัดสรรให้เฉพาะ ซึ่งแยกออกจากระบบเครือข่ายของผู้ใช้งานและติดตั้งไฟร์วอลล์ (Firewall) หรืออุปกรณ์เครือข่ายอื่นๆ เพื่อป้องกันทางเข้าเครือข่ายจากผู้ไม่หวังดี

๑.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานระบบเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

๑.๖.๑ ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก อ.ต.ก. ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือซอฟต์แวร์ในการทำ Packet Filtering ได้แก่ การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๑.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

๑.๗.๑ ติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายในลักษณะที่ผิดปกติ และมีการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๑.๗.๒ การกำหนดหมายเลข IP Address ของระบบเครือข่ายภายในต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อกับระบบเครือข่ายของ อ.ต.ก. สามารถมองเห็นโครงสร้างของระบบเครือข่ายได้โดยง่าย

๑.๗.๓ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๒.๑ ผู้ดูแลระบบ (System Administrator)

๒.๑.๑ ต้องทำการลงทะเบียนกำหนดสิทธิ์การเข้าถึงระบบเครือข่ายไร้สายของผู้ใช้งานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ดูแลระบบอนุญาตให้ผู้ใช้งานตามความจำเป็นในการใช้งานเท่านั้น

๒.๑.๒ ต้องทำการลงทะเบียนอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายไร้สาย (Wireless LAN Client) ทุกตัว

๒.๑.๓ ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์กระจายสัญญาณรั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๒.๑.๔ ต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้นที่มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

๒.๑.๕ ต้องกำหนดค่าใช้ WPA๒ (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่างอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายไร้สาย (Wireless LAN Client) และอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

๒.๑.๖ เลือกใช้วิธีการควบคุม MAC Address ร่วมกับรายชื่อผู้ใช้งานและรหัสผ่านของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะอุปกรณ์ที่มีMAC Address รายชื่อผู้ใช้งานและรหัสผ่านตามที่กำหนดไว้เท่านั้น

๒.๑.๗ ติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับระบบเครือข่ายภายในของ อ.ต.ก.

๒.๑.๘ ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ในการตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สายและเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อ ห.กส. ทราบโดยทันที

ส่วนที่ ๖
การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
(IT Operations Security)

<u>วัตถุประสงค์</u>

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการรักษาความ มั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยสารสนเทศ (IT Operation Security) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของสารสนเทศ บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

<u>แนวทางปฏิบัติ</u>

ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้องต้องกำหนดให้มีการดูแลเอกสารขั้นตอนหรือวิธีปฏิบัติงานประจำในด้านต่าง ๆ ที่สำคัญ รวมทั้งดำเนินการทบทวนและปรับปรุงขั้นตอนหรือวิธีการปฏิบัติงานให้เป็นปัจจุบันอยู่เสมอเพื่อให้บุคลากรสามารถนำไปปฏิบัติได้

๑. การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

๑.๑ ต้องจัดทำแผนการจัดการทรัพยากรระบบ (Capacity Plan) ของระบบเทคโนโลยีสารสนเทศ

๑.๒ ต้องมีการติดตามและเฝ้าระวังการใช้ทรัพยากรของระบบเทคโนโลยีสารสนเทศ

๑.๓ ต้องนำข้อมูลการเฝ้าระวัง และการวิเคราะห์ (Utilization Analysis) มาปรับปรุงแผนการจัดการทรัพยากรของระบบเทคโนโลยีสารสนเทศ

๒. การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (Server) และอุปกรณ์ที่ใช้ปฏิบัติงานของผู้ใช้เทคโนโลยีสารสนเทศ (Endpoint)

๒.๑ กำหนดกฎเกณฑ์ควบคุมการติดตั้งซอฟต์แวร์โดยผู้ใช้งาน เพื่อให้ผู้ใช้งานปฏิบัติตามโดยกำหนดรายการ Software Baseline ที่อนุญาตให้ติดตั้งและซอฟต์แวร์ที่ห้ามติดตั้ง

๒.๒ ต้องกำหนดให้มีขั้นตอนการปฏิบัติงานเพื่อควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ

๒.๓ มีมาตรการในการตรวจหา ป้องกันและกู้คืนจากโปรแกรมไม่ประสงค์ดีด้วยการติดตั้งซอฟต์แวร์ Antivirus และ Update ให้ทันสมัยอย่างสม่ำเสมอ

๒.๔ จำกัดสิทธิ์การเข้าถึงเครื่องแม่ข่ายเพื่อควบคุมให้ผู้ใช้งานสามารถใช้งานเฉพาะระบบที่ได้รับอนุญาตเท่านั้น

๒.๕ ระบบเครือข่ายทั้งหมดของ อ.ต.ก. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (IPS/IDS)

๒.๖ ติดตั้งระบบตรวจจับการบุกรุกเพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของ อ.ต.ก. ในลักษณะที่ผิดปกติ

๒.๗ หมายเลข IP Address ภายในของระบบเครือข่ายภายในของ อ.ต.ก. จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อกับระบบเครือข่ายของ อ.ต.ก. สามารถมองเห็นได้

๒.๘ จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและระบบเครือข่ายภายนอกที่สามารถระบุบนระบบเครือข่ายและต้องใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน MAC Address พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๙ ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๓. การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ของเครื่องแม่ข่าย ระบบงานและอุปกรณ์เครือข่ายที่สำคัญ

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ให้ปฏิบัติ ดังนี้

๓.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ในสื่อจัดเก็บที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

๓.๒ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า–ออกระบบ บันทึก การพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐วัน นับตั้งแต่การใช้งานสิ้นสุดลง

๓.๓ กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้

๓.๔ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริงและระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงสารสนเทศและผู้ดูแลระบบไม่ได้รับอนุญาตในการแก้ไข สารสนเทศที่เก็บรักษาไว้ยกเว้น ผู้ตรวจสอบภายในด้านระบบเทคโนโลยีสารสนเทศ (Internal IT Auditor) หรือผู้ตรวจสอบอิสระภายนอก (External IT Auditor) ที่อ.ต.ก. มอบหมาย

๓.๕ กำหนดให้มีการบันทึกการปฏิบัติงานของผู้ดูแลระบบ (Administrator Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุกได้แก่บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Logs เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วันนับตั้งแต่การใช้บริการสิ้นสุดลง

๓.๖ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๔. การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม

๔.๑ กำหนดให้มีการติดตาม ตรวจสอบ วิเคราะห์และรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ

๔.๒ ให้มีการประเมินและตัดสินใจต่อเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัยสารสนเทศ

๔.๓ ให้มีการตอบสนองต่อเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ ให้ผู้มีอำนาจสูงกว่าในการจัดการต่อเหตุละเมิดความมั่นคงปลอดภัยสารสนเทศ

๔.๔ ให้มีการรายงานสถานการณ์ด้านความมั่นคงปลอดภัยสารสนเทศให้ผู้มีอำนาจให้เร็วที่สุดเท่าที่จะทำได้

๔.๕ ให้มีการจัดเก็บข้อมูลสารสนเทศเพื่อใช้เป็นหลักฐาน เก็บไว้ในกรณีมีการละเมิดความมั่นคงปลอดภัยสารสนเทศ และต้องทำให้มั่นใจได้ว่าหลักฐานจะไม่ถูกเปลี่ยนแปลงหรือทำลาย

๕. การบริหารจัดการช่องโหว่ (Vulnerability Management) ของระบบที่เหมาะสมตามระดับความเสี่ยง

๕.๑ ให้มีกระบวนการติดตามข้อมูลเกี่ยวกับช่องโหว่ของระบบเทคโนโลยีสารสนเทศที่มีการใช้งานอย่างสม่ำเสมอ

๕.๒ ให้มีการบริหารจัดการเพื่อแก้ไขช่องโหว่ โดยการประเมินความเสี่ยงสำหรับช่องโหว่ของระบบเทคโนโลยีสารสนเทศ และกำหนดมาตรการที่เหมาะสมเพื่อจัดการกับความเสี่ยงที่เกิดจากช่องโหว่ทางเทคนิคของระบบ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

๕.๓ ติดตามและศึกษาแหล่งสารสนเทศข่าวสาร เพื่อใช้ในการติดตามช่องโหว่ของระบบเทคโนโลยีสารสนเทศของ อ.ต.ก.

๖. การทดสอบเจาะระบบ (Penetration Test)

๖.๑ ให้มีการทดสอบเจาะระบบ (Penetration Test) เพื่อพิจารณาความเสี่ยงสำหรับช่องโหว่ของระบบเทคโนโลยีสารสนเทศสำหรับระบบที่มีความสำคัญ ที่อาจทำให้ผู้ไม่หวังดีสามารถโจมตีได้โดยจัดให้มีผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระทำหน้าที่ทดสอบเจาะระบบ สม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๗. การบริหารจัดการการเปลี่ยนแปลง (Change Management)

๗.๑ ผู้ดูแลระบบต้องมีการจัดทำทะเบียนทรัพย์สินด้านระบบเทคโนโลยีสารสนเทศ

๗.๒ จัดทำบันทึกการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ โดยระบุเหตุผลของการขอเปลี่ยนแปลง รวมทั้งรายละเอียดของการดำเนินการที่เกี่ยวข้อง

๗.๓ ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ได้แก่ ผลกระทบของการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศ

๗.๔ บันทึกความเร่งด่วนของการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่ทำให้ระบบเทคโนโลยีสารสนเทศไม่สามารถให้บริการได้

๗.๕ วางแผนหรือขั้นตอนปฏิบัติสำหรับการถอยหลังกลับสำหรับกรณีที่ดำเนินการแล้วไม่สำเร็จ

๗.๖ กำหนดผู้มีอำนาจในการอนุมัติการดำเนินการ

๗.๗ กำหนดผู้มีอำนาจในการปรับปรุงหรือแก้ไขขั้นตอนปฏิบัติ

๘. การบริหารจัดการการตั้งค่าระบบ (System Configuration Management)

๘.๑ ให้มีการตั้งค่าระบบให้มีความมั่นคงปลอดภัย โดยกำหนดค่าขั้นต่ำตามมาตรฐานด้านความมั่นคงปลอดภัย (Security Baseline) ให้กับระบบเทคโนโลยีสารสนเทศที่สำคัญของ อ.ต.ก. โดยอ้างอิงจาก Center for Internet Security (CIS) หรือแหล่งข้อมูลที่น่าเชื่อถืออื่นๆ

๙. การบริหารจัดการ Patch (Patch Management)

๙.๑ จัดให้มีกระบวนการในการควบคุมการติดตั้ง patch ของระบบที่ใช้งานจริง เพื่อให้สามารถติดตั้ง patch ที่สำคัญในการรักษาความมั่นคงปลอดภัยได้อย่างทันการณ์

๑๐. การเข้ารหัสข้อมูลสารสนเทศ (Cryptography)

๑๐.๑ ข้อมูลที่สำคัญของ อ.ต.ก. ต้องกำหนดให้มีนโยบายและมาตรการการเข้ารหัสข้อมูลตามมาตรฐานสากล หรือให้สอดคล้องกับข้อตกลง ระเบียบข้อบังคับและกฎหมายที่เกี่ยวข้อง ดังนี้

๑๐.๑.๑ กำหนดให้มีการจัดประเภทของข้อมูลสารสนเทศและการสื่อสารที่จะต้องได้รับการเข้ารหัส

๑๐.๑.๒ ผู้ดูแลระบบต้องกำหนดให้มีการใช้โปรแกรมที่มีความสามารถในการเข้ารหัสข้อมูลเพื่อให้บุคลากรใช้เป็นมาตรฐานเดียวกัน โดยโปรแกรมจะต้องทำหน้าที่ในการเข้ารหัสข้อมูลอย่างเหมาะสมเมื่อมีการเชื่อมต่อผ่านระบบเครือข่ายภายในองค์กร ไปยังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายต่าง ๆ ขององค์กร

๑๐.๑.๓ ผู้ดูแลระบบต้องกำหนดให้มีการใช้โปรแกรมที่มีความสามารถในการเข้ารหัสข้อมูลเพื่อให้บุคลากรใช้เป็นมาตรฐานเดียวกัน โดยโปรแกรมจะต้องทำหน้าที่ในการเข้ารหัสข้อมูลอย่างเหมาะสมเมื่อมีการเชื่อมต่อจากเครือข่ายภายนอกองค์กรเข้ามายังเครือข่ายภายในองค์กร

๑๐.๑.๔ ผู้ดูแลระบบต้องกำหนดให้มีแนวทางการบริหารจัดการกุญแจ (Key) ที่ใช้เข้ารหัสข้อมูล เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของหน่วยงาน โดยให้มีการควบคุม กำกับติดตาม ให้ครอบคลุมตลอดทั้งวงจรในการนำกุญแจรหัสลับ ไปใช้งาน ได้แก่ การสร้างกุญแจรหัสลับการจัดเก็บและดูแลรักษากุญแจรหัสลับ การนำกุญแจรหัสลับไปใช้ การกำหนดอายุของกุญแจรหัสลับ ตลอดจนการทำลายกุญแจรหัสลับเมื่อไม่ได้ใช้งาน

๑๑. การใช้บริการคอมพิวเตอร์เสมือน (Cloud Computing)

๑๑.๑ ต้องกำหนดกลยุทธ์และนโยบายการใช้บริการ Cloud Computing สำหรับผู้ให้บริการภายนอก

๑๑.๒ ต้องมีแนวทางในการบริหารความเสี่ยงที่เกี่ยวข้องกับการใช้บริการ Cloud Computing

๑๑.๓ ต้องมีการบริหารจัดการผู้ให้บริการ Cloud Computing จากภายนอก

๑๑.๔ ต้องมีการรักษาความปลอดภัยและความลับของระบบงานและข้อมูลของการใช้บริการ Cloud Computing

๑๑.๕ ต้องมีการดำเนินการเพื่อให้มั่นใจว่าระบบงานและข้อมูลของการใช้บริการ Cloud Computing มีความถูกต้องเชื่อถือได้

๑๑.๖ ต้องมีการดำเนินการเพื่อให้มั่นใจถึงความพร้อมใช้ของการใช้บริการ Cloud Computing

๑๑.๗ ต้องมีการดำเนินการเกี่ยวกับการคุ้มครองที่ครอบคุลถึงผู้ใช้บริการของ อ.ต.ก.

๑๒. การตรวจสอบระบบสารสนเทศ (Information Systems Audit Considerations)

๑๒.๑ หน่วยงานที่รับผิดชอบด้านการตรวจสอบภายใน ต้องจัดทำแผนการตรวจสอบระบบสารสนเทศและขั้นตอนการปฏิบัติงานการตรวจสอบระบบสารสนเทศ

๑๒.๒ หน่วยงานที่รับผิดชอบด้านการตรวจสอบภายใน ต้องตรวจสอบตามแผนการตรวจสอบระบบสารสนเทศ ทั้งนี้ต้องจัดทำเอกสารสำหรับบันทึกผลการตรวจสอบการปฏิบัติงานเพื่อใช้อ้างอิงผลการตรวจสอบ นอกจากนี้ในกรณีที่ต้องเข้าถึงระบบงานที่ให้บริการจริง จะต้องมีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging Record) การเข้าระบบและกิจกรรมในระหว่างการตรวจสอบ

ส่วนที่ ๗
การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ
(System Acquisition and Development)

วัตถุประสงค์

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ (System Acquisition and Development) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของสารสนเทศ บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

แนวทางปฏิบัติ

๑. การระบุความต้องการในการจัดหาและการพัฒนาระบบสารสนเทศ (Security Requirements of Information Systems)

๑.๑ การพัฒนาระบบเทคโนโลยีสารสนเทศของกองเทคโนโลยีและสารสนเทศ ต้องควบคุมให้มีการกำหนดความต้องการด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศที่จะถูกพัฒนาขึ้นใหม่หรือในการปรับปรุงระบบเทคโนโลยีสารสนเทศเดิม เพื่อให้ผู้พัฒนานำความต้องการด้านความมั่นคงปลอดภัยนั้นไปใช้ในการวิเคราะห์และออกแบบระบบเทคโนโลยีสารสนเทศให้เกิดความมั่นคงปลอดภัยในการใช้งาน

๑.๒ กรณีที่ระบบเทคโนโลยีสารสนเทศที่พัฒนาขึ้นใหม่หรือที่ได้รับการปรับปรุงเป็นระบบเทคโนโลยีสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ เจ้าหน้าที่ผู้ที่ควบคุมการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศนั้น ต้องพิจารณาและกำหนดมาตรการทางเทคนิคในการป้องกันเหตุการณ์

๒. พัฒนาระบบอย่างมั่นคงปลอดภัย (Security in Development Process)

๒.๑ การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลให้การเปลี่ยนแปลงที่เกิดขึ้นระหว่างการดำเนินงานพัฒนาระบบอย่างเป็นกระบวนการ โดยให้การเปลี่ยนแปลงที่เกิดขึ้นระหว่างการพัฒนาระบบ ต้องเข้าสู่ขั้นตอนการบริหารการเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ

๒.๒ การเปลี่ยนแปลงระบบปฏิบัติการของระบบเทคโนโลยีสารสนเทศใดๆ เจ้าหน้าที่ผู้ที่ควบคุมการดำเนินงานต้องกำหนดให้มีการทบทวนและทดสอบการทำงานของระบบเทคโนโลยีสารสนเทศเพื่อให้แน่ใจว่าระบบเทคโนโลยีสารสนเทศสามารถทำงานได้ตามปกติ

๒.๓ การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ ต้องควบคุมดูแลไม่ให้มีการเปลี่ยนแปลงแก้ไข Software Package โดยไม่ได้รับอนุญาต และหากจำเป็นต้องแก้ไขให้จำกัดการแก้ไข Software Package นั้นเท่าที่จำเป็น พร้อมทั้งต้องทำการสำรอง Software Package นั้นก่อนดำเนินการแก้ไข

๒.๔ การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ ต้องนำหลักการวิศวกรรมสำหรับการพัฒนาระบบให้เกิดความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศของกองเทคโนโลยีและสารสนเทศ

๒.๕ การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ ต้องควบคุมให้การดำเนินงานพัฒนาระบบเทคโนโลยีสารสนเทศอยู่ในบริเวณที่มีความมั่นคงปลอดภัยตามที่กองเทคโนโลยีและสารสนเทศกำหนด เพื่อป้องกันความเสี่ยงจากผู้ที่ไม่มีส่วนเกี่ยวข้องกับการพัฒนาระบบเข้าถึงสารสนเทศ ระบบสนับสนุนและอุปกรณ์ เครื่องมือต่าง ๆ ที่ใช้ในการพัฒนาระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๒.๖ กรณีที่ อ.ต.ก. ไม่ได้เป็นผู้พัฒนาระบบเทคโนโลยีสารสนเทศเอง ให้เจ้าหน้าที่ผู้ที่ควบคุมการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศนั้น ต้องจัดทำสัญญาจ้างตามกระบวนการจัดซื้อจัดจ้างของ อ.ต.ก. รวมทั้งต้องกำกับและติดตามการดำเนินงานของผู้รับจ้างอย่างเหมาะสมตามกิจกรรมและระยะเวลาที่ถูกกำหนดไว้

๒.๗ การจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการทดสอบการทำงานของฟังก์ชั่นในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ตั้งแต่ระบบเทคโนโลยีสารสนเทศนั้นอยู่ระหว่างการพัฒนาหรืออยู่ระหว่างการปรับปรุงเปลี่ยนแปลง เพื่อให้มั่นใจว่าฟังก์ชั่นในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศสามารถทำงานได้ตามความต้องการ

๓. การปกป้องข้อมูลที่นำไปใช้ในการทดสอบระบบ (Security in Test Data)

๓.๑ ผู้ดูแลระบบและผู้พัฒนาระบบ ต้องควบคุมให้มีการเลือกชุดข้อมูลสารสนเทศที่จะนำไปใช้เพื่อการทดสอบในระบบสารสนเทศอย่างระมัดระวัง รวมทั้งมีแนวทางควบคุมและป้องกันข้อมูลรั่วไหล

๓.๒ กำหนดให้มีการควบคุมการเข้าถึง การใช้งาน การจัดเก็บ และทำลายข้อมูลที่ใช้ในการทดสอบ เพื่อป้องกันการรั่วไหล ที่อาจเกิดขึ้นและถูกเข้าถึงโดยไม่ได้รับอนุญาต

๓.๓ ผู้ดูแลระบบ ต้องแยกระบบสารสนเทศสำหรับการพัฒนา ทดสอบ และใช้งานจริงออกจากกันเพื่อลดความเสี่ยงในการเข้าใช้งานหรือการเปลี่ยนแปลงระบบสารสนเทศโดยมิได้รับอนุญาต

ส่วนที่ ๘
การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ
(IT Incident and Problem Management)

วัตถุประสงค์

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident and Problem Management) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของสารสนเทศ บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

แนวทางปฏิบัติ

๑. การบริหารจัดการเหตุการณ์ผิดปกติและปัญหาด้านเทคโนโลยีสารสนเทศ

๑.๑ ให้มีการบันทึกจัดเก็บข้อมูลและรายงานอุบัติการณ์เกี่ยวกับเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ผ่านช่องทางบริหารจัดการที่กำหนดไว้อย่างเหมาะสมและรวดเร็วทันการณ์

๑.๒ ให้มีการบันทึกและรายงานช่องโหว่หรือจุดอ่อนใด ๆ ด้านเทคโนโลยีสารสนเทศ ที่อาจสังเกตพบระหว่างการใช้งานระบบสารสนเทศผ่านช่องทางบริหารจัดการที่กำหนดไว้อย่างเหมาะสม

๑.๓ กำหนดขอบเขตความรับผิดชอบของผู้มีส่วนเกี่ยวข้อง และขั้นตอนการปฏิบัติงานเพื่อตอบสนองต่อสถานการณ์ด้านเทคโนโลยีสารสนเทศที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด อย่างรวดเร็ว มีระเบียบ และมีประสิทธิผล

๑.๔ ผู้ดูแลระบบ และผู้ให้บริการภายนอก ที่ทำหน้าที่แก้ไขอุบัติการณ์ด้านเทคโนโลยีสารสนเทศ ต้องดำเนินการรวบรวม จัดเก็บ และนำเสนอหลักฐาน ให้สอดคล้องกับหลักเกณฑ์ของกฎหมายที่ใช้บังคับ หากมีขั้นตอนการติดตามผลกับบุคคลหรือหน่วยงานภายหลังจากเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ซึ่งเกี่ยวข้องกับการดำเนินการทางกฎหมาย (ไม่ว่าทางแพ่งหรือ ทางอาญา)

๑.๕ ผู้ดูแลระบบ ต้องดำเนินการตรวจสอบและประเมินช่องโหว่หรือจุดอ่อนใดๆ ด้านเทคโนโลยีสารสนเทศ จัดแยกกลุ่มและลำดับความสำคัญตามเกณฑ์ที่องค์กรกำหนด และแจ้งผู้ที่เกี่ยวข้องเพื่อแก้ไขในกรณีที่พบว่าช่องโหว่หรือจุดอ่อนนั้นเป็นอาจเป็นอุบัติการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๑.๖ ผู้ดูแลระบบ และผู้ให้บริการภายนอก ที่ทำหน้าที่แก้ไขอุบัติการณ์ด้านเทคโนโลยีสารสนเทศ ต้องดำเนินการตามขั้นตอนการปฏิบัติงานที่ได้กำหนดไว้

๑.๗ ให้มีการวิเคราะห์ข้อมูลและแนวโน้มเกี่ยวกับเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ

๑.๘ ให้มีการระบุปัญหาเพื่อยกระดับในการวิเคราะห์หาสาเหตุที่แท้จริง รวมทั้งกำหนดการดำเนินการในการป้องกันการเกิดซ้ำของเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศเหล่านั้น

๑.๙ ให้มีการวิเคราะห์เพื่อหาสาเหตุที่แท้จริง (Root Cause) ของเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศนั้น และดำเนินการแก้ไขให้เหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศดังกล่าวไม่เกิดขึ้นซ้ำ

๒. การรับมือเหตุการณ์ผิดปกติทางไซเบอร์

๒.๑ ต้องมีมาตรการในการเตรียมความพร้อมสำหรับเหตุการณ์ด้านความปลอดภัยไซเบอร์ (Preparing for a Cyber Security Incident)

๒.๒ ต้องมีมาตรการในการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ (Responding to Cyber Security Incident)

๒.๓ ต้องมีการติดตามสถานการณ์ด้านความปลอดภัยทางไซเบอร์ (Following up the Cyber Security Incident)

ส่วนที่ ๙
การจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

<u>วัตถุประสงค์</u>

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของสารสนเทศ บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

<u>แนวทางปฏิบัติ</u>

๑. การพิจารณาระบบเทคโนโลยีสารสนเทศที่สำคัญ

๑.๑ จัดทำบัญชีระบบเทคโนโลยีสารสนเทศและกำหนดลำดับความสำคัญ

๑.๒ กำหนดวิธีการและความถี่ของการสำรองข้อมูลที่เหมาะสมให้อยู่ในสภาพพร้อมใช้ตามที่ อ.ต.ก. กำหนด

๒. การจัดทำแผนความต่อเนื่องทางธุรกิจ (BCP)

เพื่อเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์และปรับปรุงให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับภารกิจของ อ.ต.ก. ตามแนวทางต่อไปนี้

๒.๑ ประเมินความเสี่ยงสำหรับระบบเทคโนโลยีสารสนเทศที่มีความสำคัญและกำหนดมาตรการเพื่อลดความเสี่ยง ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง การปิดล้อมพื้นที่จนทำให้ไม่สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศได้

๒.๒ กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล การกู้คืนระบบ และการทดสอบการกู้คืนระบบเทคโนโลยีสารสนเทศ

๒.๓ กำหนดช่องทางการติดต่อกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการระบบสำรองข้อมูล ผู้ให้บริการเครือข่าย หรือ ผู้ให้บริการคลาวด์

๓. การกำหนดหน้าที่และความรับผิดชอบ

๓.๑ ผู้ที่เกี่ยวข้องในการจัดทำและการทบทวนแผนความต่อเนื่องทางธุรกิจ (BCP-IT)

๓.๒ ผู้ดูแลระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย และระบบสำรองข้อมูล

๓.๓ ผู้ที่เกี่ยวข้องทั้งหมดตามแผนผังสายการบังคับบัญชา (Lines of Authority) เมื่อเกิดสถานการณ์ฉุกเฉิน

๔. การฝึกซ้อม

ดำเนินการฝึกซ้อมตามแผนความต่อเนื่องทางธุรกิจ (BCP-IT) เพื่อทดสอบสภาพความพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศและระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๕. การทบทวน

๕.๑ ทบทวนและปรับปรุงแผนความต่อเนื่องทางธุรกิจ (BCP-IT) ให้เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้และสามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับภารกิจของ อ.ต.ก. อย่างน้อยปีละ ๑ ครั้ง

๕.๒ ให้ความรู้และสร้างความตระหนักหรือแก่เจ้าหน้าที่หรือผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุฉุกเฉิน

๕.๓ ควบคุมให้มีการประเมินความต้องการด้านการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบที่มีความสำคัญสูง และกำกับให้การติดตั้งอุปกรณ์หรือระบบเพื่อรักษาความต่อเนื่องในการดำเนินงาน (Redundancy) ที่เหมาะสม

๖. การจัดทำระบบสำรองและกู้คืนข้อมูล

๖.๑ การคัดเลือกการสำรองข้อมูล

ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตามแนวทางต่อไปนี้

๖.๑.๑ ต้องสำรองข้อมูลสำคัญทางธุรกิจ รวมถึง โปรแกรมระบบปฏิบัติการ (operating system) โปรแกรมระบบงานคอมพิวเตอร์ (application system) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้ งานได้อย่างต่อเนื่อง

๖.๑.๒ ควรมีขั้นตอนหรือวิธีปฏิบัติในการสำรองข้อมูล เพื่อเป็นแนวทางให้แก่ ผู้ปฏิบัติงาน โดย อย่างน้อยควรมีรายละเอียด ดังนี้

๖.๑.๒.๑ ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง

๖.๑.๒.๒ ประเภทสื่อบันทึก (media)

๖.๑.๒.๓ จำนวนที่ต้องสำรอง (copy)

๖.๑.๒.๔ ขั้นตอนและวิธีการสำรองโดยละเอียด

๖.๑.๒.๕ สถานที่และวิธีการเก็บรักษาสื่อบันทึก

๖.๑.๓ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบ สารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๖.๑.๔ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการ สำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มี วิธีการสำรองข้อมูลดังนี้

๖.๑.๔.๑ กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้และความถี่ในการสำรอง

๖.๑.๔.๒ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือ การสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๖.๑.๕ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูล ที่สำรองสำเร็จ/ไม่สำเร็จ เป็นต้น

๖.๑.๖ ตรวจสอบข้อมูลทั้งหมดของระบบว่า มีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ ต่างๆที่เกี่ยวข้องกับระบบสารสนเทศข้อมูลการตั้งค่า (Configuration) ข้อมูลในฐานข้อมูล เป็นต้น

๖.๑.๗ จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูลโดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้น ให้สามารถ แสดงถึงระบบซอฟต์แวร์ วันที่เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๖.๑.๘ ในกรณีจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรอง กับหน่วยงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติ กับหน่วยงาน เช่น ไฟไหม้ เป็นต้น
ตามปกติ

๖.๑.๙ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๖.๑.๑๐ ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้

๖.๑.๑๑ ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ต้องคำนึงถึงวิธีการนำข้อมูลกลับมา ใช้งานในอนาคตด้วย เช่น ถ้าจัดเก็บข้อมูลในสื่อบันทึกประเภทใด ก็ต้องมีการเก็บอุปกรณ์และซอฟท์แวร์ที่ เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

๖.๑.๑๒ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้ ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๖.๑.๑๓ กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๖.๒ การสำรองและกู้คืนข้อมูล

เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูลและสามารถนำข้อมูลกลับมาใช้งานได้ในกรณีที่ฮาร์ดดิสก์เสียหาย ไวรัสคอมพิวเตอร์ทำลายข้อมูล ผู้บุกรุกทำการลบข้อมูลหรือเปลี่ยนแปลงข้อมูล การเผลอลบข้อมูลหรือเปลี่ยนแปลงข้อมูลโดยผู้ใช้งานเอง โดยมีมาตรการ ดังนี้

๖.๒.๑ การสำรองข้อมูล

๖.๒.๑.๑ ผู้ดูแลระบบต้องตั้งค่าระบบให้สำรองข้อมูลโดยอัตโนมัติ หรือทำการสำรองข้อมูล ของระบบซึ่งอยู่ในความรับผิดชอบของตนเอง ตามความเหมาะสมของแต่ละระบบ ไม่น้อยกว่า ๑ ครั้งต่อเดือน

๖.๒.๑.๒ ผู้ดูแลระบบต้องตั้งค่าสำรองข้อมูลอัตโนมัติสำหรับเครื่องคอมพิวเตอร์แม่ข่ายของเว็บไซต์ (Web Server)

๖.๒.๑.๓ ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไปจะต้องทำการสำรองข้อมูลในเครื่องคอมพิวเตอร์ของตนเองตามความเหมาะสม ไม่น้อยกว่า ๑ ครั้งต่อเดือน

๖.๒.๑.๔ เมื่อองค์กรประกาศให้มีการสำรองข้อมูล เนื่องจากจะมีการดำเนินการที่อาจ ส่งผลต่อข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้ ผู้ใช้จะต้องทำการสำรองข้อมูลดังกล่าว ภายในระยะเวลาที่กำหนด

๖.๒.๑.๕ หากผู้ดูแลระบบหรือผู้ใช้งานเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใดเป็นข้อมูลสำคัญให้พิมพ์ (Print) ออกมาเก็บสำรองไว้ในรูปของเอกสารกระดาษ (Hard Copy)

๖.๒.๑.๖ แผนกผู้ดูแลระบบต้องทำการทดสอบกู้ข้อมูลสำรองในทุกระบบโดยต้องมีการทดสอบ อย่างน้อยปีละ ๑ ครั้ง การทดสอบดังกล่าวต้องใช้ข้อมูลสำรองจากระบบที่ใช้งานจริง แต่ทดสอบบนระบบทดสอบ

๖.๒.๑.๗ ผู้ดูแลระบบต้องทำการสำรองข้อมูลอิเล็กทรอนิกส์ขององค์กร และเก็บรักษาไว้ ตามแนวทางปฏิบัติการเก็บรักษาข้อมูลขององค์กร โดยกำหนดระยะเวลาในการเก็บรักษาข้อมูลที่สำคัญด้วย

๖.๒.๒ การกู้คืนข้อมูล

เพื่อให้การฟื้นฟูระบบ/ข้อมูลจากความเสียหายที่อาจเกิดขึ้น จากการหยุดทางานของการประมวลผลโปรแกรม (Hang) หรือไฟฟ้าดับ ตลอดจน เหตุการณ์อื่นใดซึ่งส่งผลต่อเครื่องคอมพิวเตอร์ หรือการ ประมวลผลของคอมพิวเตอร์หยุดทำงานอย่างกะทันหันหรือเปลี่ยนการทำงานไปจากเดิม ทำให้ไม่สามารถบันทึก ข้อมูลได้ทันเวลาหรือไม่สามารถใช้งานคอมพิวเตอร์ได้ตามปกติมีมาตรการในการกู้คืนข้อมูลดังนี้

๖.๒.๒.๑ ผู้ใช้งานต้องเปิดใช้งานการกู้คืน (Recovery) ของระบบปฏิบัติการตลอดเวลา

๖.๒.๒.๒ ผู้ดูแลระบบต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟต์แวร์ใหม่เพื่อทดแทนของเดิมที่เสียหาย

๖.๒.๒.๓ ผู้ดูแลระบบต้องทำการบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์สนับสนุน เพื่อ ป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

ส่วนที่ ๑๐
การบริหารจัดการผู้ให้บริการภายนอก
(Third Party Management)

<u>วัตถุประสงค์</u>

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้ให้บริการภายนอก บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

<u>แนวทางปฏิบัติ</u>

๑. การบริหารจัดการข้อตกลงการให้บริการ (Service Level Agreement - SLA) และข้อตกลงด้านการรักษาความลับของข้อมูล (Non-Disclosure Agreement - NDA)

๑.๑ การจัดจ้างผู้ให้บริการภายนอกเพื่อเข้ามาดำเนินงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ กองเทคโนโลยีและสารสนเทศต้องมีการกำหนดและข้อตกลงการให้บริการ (SLA) และข้อตกลงด้านการรักษาความลับของข้อมูล (NDA) ไว้ในเอกสารจัดจ้างหรือสัญญา

๑.๒ กำหนดให้มีการติดตาม ทบทวน และตรวจประเมินการให้บริการของผู้ให้บริการภายนอกให้สอดคล้องข้อกำหนดการจ้าง (SLA) กับระยะเวลาในการจ้างผู้ให้บริการภายนอกรายนั้น ๆ ซึ่งการติดตามและทบทวนการให้บริการของผู้ให้บริการภายนอกเพื่อทำให้มั่นใจว่าผู้ให้บริการภายนอกยังคงปฏิบัติตามข้อตกลงการให้บริการ (SLA) และเงื่อนไขที่ได้ระบุไว้ในข้อตกลง

๒. การควบคุมหน่วยงานภายนอกเข้าถึงระบบดิจิทัลและสารสนเทศ

๒.๑ ควรกำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการ และคัดเลือกผู้ให้บริการที่มีขั้นตอนการปฏิบัติงานที่รอบคอบรัดกุมและเป็นที่น่าเชื่อถือ

๒.๒ ควรมีสัญญาที่ระบุเกี่ยวกับการรักษาความลับของข้อมูล (data confidentiality) และขอบเขตงาน และเงื่อนไขในการให้บริการ (service level agreement) อย่างชัดเจน

๒.๓ บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบดิจิทัลและสารสนเทศขององค์การตลาดเพื่อเกษตรกร จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการสำนักดิจิทัลและสารสนเทศ หรือผู้อำนวยการองค์การตลาดเพื่อเกษตรกร

๒.๔ ในกรณีที่ใช้บริการด้านการพัฒนาระบบงาน ต้องกำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้ สำหรับการพัฒนาระบบงาน (develop environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (production environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้ มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ เช่น ให้พนักงานสำนักดิจิทัลและสารสนเทศควบคุมดูแลการทำงานของผู้ ให้บริการอย่างใกล้ชิด ในกรณีที่ผู้ให้บริการมาปฏิบัติหน้าที่ที่องค์การตลาดเพื่อเกษตรกรฯ (Onsite service) และให้เจ้าหน้าที่สำนักดิจิทัลและสารสนเทศตรวจสอบการ

ทำงานของผู้ให้บริการอย่างละเอียด ในกรณีที่เป็นการให้บริการในลักษณะ remote access และปิดการเชื่อมต่อทันทีที่การให้บริการเสร็จสิ้น เป็นต้น

๒.๕ ผู้ดูและระบบต้องควบคุมการปฏิบัติงานและการเข้าถึงข้อมูลที่มีความสำคัญขององค์การตลาดเพื่อเกษตรกร ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และ การรักษาความพร้อมให้บริการ (Availability)

๒.๖ ควรดำเนินการให้ผู้ให้บริการจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

๒.๗ ควรกำหนดให้ผู้ให้บริการรายงานการปฏิบัติงาน ปัญหาต่าง ๆ และแนวทางแก้ไข

๒.๘ ควรมีขั้นตอนในการตรวจรับงานของผู้ให้บริการ และนำเสนอต่อผู้บังคับบัญชา

ส่วนที่ ๑๑
การป้องกันโปรแกรมไม่ประสงค์ดี
(Malicious Software Prevention)

<u>วัตถุประสงค์</u>

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการป้องกันโปรแกรมไม่ประสงค์ดี (Malicious Software Prevention) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้ให้บริการภายนอก บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

<u>แนวทางปฏิบัติ</u>

๑. การป้องกันโปรแกรมไม่ประสงค์ดี

๑.๑ ห้ามมีการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่น ที่ อ.ต.ก. ไม่อนุญาตให้ใช้งาน

๑.๒ ให้ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่ประสงค์ดีให้กับระบบเทคโนโลยีสารสนเทศของ อ.ต.ก.

๑.๓ ให้ผู้ดูแลระบบดำเนินการตรวจสอบโปรแกรมไม่ประสงค์ดีในเครื่องเซิร์ฟเวอร์ให้บริการและอุปกรณ์ เทคโนโลยีสารสนเทศอื่น ๆ ณ จุดทางเข้า-ออกเครือข่ายอย่างสม่ำเสมอ เพื่อดักจับโปรแกรมไม่ประสงค์ดีที่เข้าสู่ระบบ

๑.๔ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์การจัดการ การกู้คืนระบบจากความเสียหายที่พบ เป็นต้น

๑.๕ มีการติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

๑.๖ ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๑.๗ เครื่องคอมพิวเตอร์ทั้งหมด ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และ เครื่องคอมพิวเตอร์แบบพกพา (Notebook) ต้องได้รับการติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัสรุ่นล่าสุดของ อ.ต.ก. จากเจ้าหน้าที่กองเทคโนโลยีและสารสนเทศ และจะต้องเปิดใช้งานโปรแกรมตรวจสอบและกำจัดไวรัสตลอดเวลา

๑.๘ เครื่องคอมพิวเตอร์ Server ที่ให้บริการการตรวจสอบและกำจัดไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุด ของไวรัสอยู่เสมอ และต้องเป็นผู้ให้บริการปรับปรุงข้อมูลไวรัสล่าสุดให้แก่เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ และเครื่องคอมพิวเตอร์แบบพกพาทุกเครื่องโดยอัตโนมัติ

๑.๙ ต้องทำการตรวจสอบไวรัสกับแฟ้มข้อมูล (File) ต่าง ๆ ที่ download มา แฟ้มข้อมูลที่แนบมากับ ไปรษณีย์อิเล็กทรอนิกส์, แฟ้มข้อมูลที่ได้มาจากสื่อบันทึกข้อมูลภายนอก (CD, Thumb Drive, Diskette or Share File)

๑.๑๐ กองเทคโนโลยีและสารสนเทศ ต้องกำหนดให้เครื่องลูกข่ายทุกเครื่องในสำนักงาน อ.ต.ก. ทำการตรวจสอบไวรัส (Scan Virus) โดยอัตโนมัติในเวลาที่กำหนดเป็นประจำทุกวัน ดังนั้นต้องแจ้งให้ผู้ใช้งานเปิดเครื่องคอมพิวเตอร์เพื่อทำการตรวจสอบไวรัสในเวลาดังกล่าว

ส่วนที่ ๑๒
การรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ท
(Website and Internet Security)

<u>วัตถุประสงค์</u>

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ท (Website and Internet Security) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ตระหนักถึงการปกป้อง รับมือ และลดความเสี่ยงการโจมตีทางด้านไซเบอร์ พร้อมทั้งเพื่อให้ผู้ใช้บริการสามารถใช้เว็บไซต์และเว็บแอปพลิเคชันได้อย่างปลอดภัยและมีการคุ้มครองข้อมูลส่วนบุคคลของผู้ใช้บริการอย่างเหมาะสมและเพียงพอ

๓. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้องทราบกฎเกณฑ์แนวทางปฏิบัติการใช้งานอินเตอร์เน็ทอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้งานระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของ อ.ต.ก. ถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

<u>แนวทางปฏิบัติ</u>

๑. การรักษาความมั่นคงปลอดภัยเว็บไซต์และเว็บแอปพลิเคชั่น

๑.๑ เครื่องคอมพิวเตอร์แม่ข่ายให้บริการเว็บไซต์และเว็บแอปพลิเคชั่น ให้มีการตรวจสอบช่องโหว่และมาตรการปกป้องการโจมตีทางด้านไซเบอร์จากผู้ไม่ประสงค์ดี

๑.๒ มีการออกแบบระบบเครือข่ายและติดตั้งระบบไฟร์วอลล์ (Firewall) เพื่อป้องกันการโจมตีจากผู้ไม่ประสงค์ดีที่พยายามโจมตีข้อมูลและระบบการให้บริการของเว็บไซต์และเว็บแอปพลิเคชั่น

๑.๓ มีการกำหนดขั้นตอนพัฒนาเว็บไซต์และเว็บแอปพลิเคชั่น (Secure Coding) ให้มีความมั่นคงปลอดภัย

๑.๔ มีการควบคุมและจำกัดจำนวนการเข้าถึง (Session) เว็บไซต์และเว็บแอปพลิเคชั่น และกำหนดระยะเวลาการควบคุมการเข้าถึง (Session Time - Out)

๑.๕ มีการกำหนดมาตรการเข้ารหัสและตรวจสอบสิทธิ์ผ่านมาตรฐานความปลอดภัย (Hypertext Transfer Protocol Secure : HTTPS) เพื่อการปกป้องข้อมูลของผู้ใช้บริการเว็บไซต์และเว็บแอปพลิเคชั่น

๑.๖ มีการจำกัดการเข้าถึงและใช้งานระบบสารสนเทศตามสิทธิ์ของผู้ใช้งาน

๑.๗ มีการจัดเก็บ Log Files เพื่อการป้องกันการบุกรุกจากผู้ไม่ประสงค์ดีตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๑.๘ มีการเก็บรวบรวมและใช้คุกกี้ (Cookies) ที่จำเป็นเพื่อความสะดวกและรวดเร็วในการให้บริการเว็บไซต์และเว็บแอพพลิเคชันที่อยู่ภายใต้ความดูแลของกองเทคโนโลยีและสารสนเทศ ซึ่งคุกกี้ที่เก็บนั้นเป็นการเก็บข้อมูลชั่วคราวที่จำเป็นลงในเครื่องคอมพิวเตอร์ของผู้ใช้บริการโดยเจ้าของข้อมูลส่วนบุคคลสามารถตั้งค่าหรือลบการใช้งานคุกกี้ได้ด้วยตนเอง

๑.๙ มีการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) บนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการและอัปเดตโปรแกรม ดังกล่าวอยู่เสมอ

๒. การรักษาความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ท

๒.๑ ผู้ใช้งานจะต้องใช้งานอินเตอร์เน็ทที่กำหนดและจัดสรรโดย อ.ต.ก. เท่านั้น ซึ่งจะเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ อ.ต.ก. จัดสรรไว้ เช่น Proxy Firewall IP-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial – Up Modem หรือ โทรศัพท์มือถือ ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจาก ห.กส. เป็นลายลักษณ์อักษร ก่อนการดำเนินการ

๒.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

๒.๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเตอร์เน็ทจะต้องมีการตรวจสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งและใช้งานข้อมูลทุกครั้ง

๒.๔ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเตอร์เน็ทของ อ.ต.ก. เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๒.๕ ผู้ใช้งานจะถูกกำหนดสิทธิ์โดยผู้ดูแลระบบในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ อ.ต.ก.

๒.๖ ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ อ.ต.ก.

๒.๗ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเตอร์เน็ท

๒.๘ ผู้ใช้งานต้องตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเตอร์เน็ทก่อนนำข้อมูลไปใช้งาน

๒.๙ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ อ.ต.ก. ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๒.๑๐ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเตอร์เน็ท ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สิ้นทางปัญญา

๒.๑๑ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ อ.ต.ก.

๒.๑๒ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ (Webboard) ผู้ใช้งานต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงานการทำลายความสัมพันธ์กับบุคคลากรของหน่วยงานอื่นๆ

๒.๑๓ หลังจากใช้งานอินเตอร์เน็ทเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๒.๑๔ ผู้ละเมิดนโยบายความมั่นคงปลอดภัยของการใช้งานอินเตอร์เน็ทจะถูกระงับการใช้งานอินเตอร์เน็ททันที หรือจนกว่าจะได้รับอนุญาตจาก ห.กส.

ส่วนที่ ๑๓
การประเมินความเสี่ยง
(Risk Assessment Policy)

<u>วัตถุประสงค์</u>

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการประเมินความเสี่ยง (Risk Assessment Policy) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของข้อมูล บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึง และใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

๓. เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้ง ให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้ อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

<u>แนวทางปฏิบัติ</u>

๑. การประเมินความเสี่ยง

๑.๑ ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงขององค์กร เพื่อการตรวจสอบและประเมินความเสี่ยงนั้น ดังต่อไปนี้

๑.๑.๑ ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการ เพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

๑.๑.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สาย โดยไม่ได้รับอนุญาต

๑.๑.๓ ความเสี่ยงที่เกิดจากเครื่องมือด้านดิจิทัลและสารสนเทศ หรือระบบเครือข่ายเกิดความขัดข้องระหว่างการใช้งาน

๑.๑.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกัน มากกว่าหนึ่งจุด

๑.๑.๕ ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่น โดยไม่ได้รับอนุญาต

๑.๑.๖ จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑.๒ กำหนดวิธีการในการตรวจสอบและประเมินความเสี่ยง และความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๑.๓ การตรวจสอบและประเมินความเสี่ยงให้คำนึงองค์ประกอบ ดังต่อไปนี้

๑.๓.๑ ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๑.๓.๓ จุดอ่อนด้านความปลอดภัยของระบบอาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๑.๓.๔ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในสำนักงาน เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ ความเสียหายหรืออันตรายที่จะเกิดขึ้นของหน่วยงาน

ส่วนที่ ๑๔
การกำหนดผู้รับผิดชอบ
(Responsibility Policy)

<u>วัตถุประสงค์</u>

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการกำหนดผู้รับผิดชอบ (Responsibility Policy) ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของข้อมูล บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึง และใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

๓. การกำหนดผู้รับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตาม แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

<u>แนวทางปฏิบัติ</u>

๑. ระดับนโยบาย

๑.๑ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้น

๑.๒ ผู้บริหารดิจิทัลและสารสนเทศระดับสูง (Chief Information officer : CIO) มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานที่ทำหน้าที่ และผู้อำนวยการสำนักดิจิทัลและสารสนเทศ เป็นผู้รับผิดชอบ ในการสั่งการตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ติดตามและกำกับดูแล ควบคุมตรวจสอบ รวมทั้ง ให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติ

๒. ระดับผู้บริหาร

๒.๑ หัวหน้ากองเทคโนโลยีและสารสนเทศ รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงานอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ความเสี่ยง ของระบบฐานข้อมูลและสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยง และตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการดังนี้

๒.๑.๒ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ระบบคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมด ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม.

๒.๑.๓ แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ และ ระบบเครือข่ายขององค์การตลาดเพื่อเกษตรกรสารสนเทศ

๒.๑.๔ กำกับดูแลเกี่ยวกับงานสารสนเทศ และงานต่าง ๆ ของกองเทคโนโลยีและสารสนเทศ

๒.๑.๕ รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับระดับสูงทราบอย่างสม่ำเสมอ

๓. ระดับปฏิบัติ

ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากผู้บังคับบัญชา หรือ หัวหน้ากองเทคโนโลยีและสารสนเทศ เช่น เจ้าหน้าที่คอมพิวเตอร์ และ ลูกจ้างกองเทคโนโลยีและสารสนเทศ

๓.๑ ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๒ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศ จากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๓.๓ รับผิดชอบควบคุมดูแลรักษาความปลอดภัยและบำรุงรักษาระบบเครื่องคอมพิวเตอร์ระบบเครือข่าย ห้องคอมพิวเตอร์แม่ข่ายและเครือข่าย

๓.๔ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๓.๕ ป้องกันและแก้ไขปัญหาการถูกเจาะระบบ (Hack) เข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๓.๖ รับผิดชอบในการรักษาความปลอดภัยระบบอินเตอร์เน็ต

๓.๗ ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การตลาดเพื่อเกษตรกร

ส่วนที่ ๑๕

การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

<u>วัตถุประสงค์</u>

๑. เพื่อให้ อ.ต.ก. มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ ของ อ.ต.ก.

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูง ผู้บริหาร ผู้ดูแลระบบ เจ้าหน้าที่ หน่วยงานเจ้าของข้อมูล บุคคลภายนอกที่ปฏิบัติงานให้กับ อ.ต.ก. และบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึง และใช้งานสารสนเทศของ อ.ต.ก. รับทราบและทำความเข้าใจ รวมทั้งปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด

๓. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานขององค์กร

๔. เพื่อป้องกันการกระทำที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน

๕. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์มีความมั่นคงปลอดภัยมากขึ้น

<u>แนวทางปฏิบัติ</u>

๑. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศอย่างน้อย ปีละ ๑ ครั้ง หรือจัดให้มีคู่มือความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๒. จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางระบบอินทราเน็ตขององค์การตลาดเพื่อเกษตรกร

๓. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

ระเบียบปฏิบัติงาน
ระเบียบปฏิบัติด้านเทคโนโลยีสารสนเทศองค์การตลาดเพื่อเกษตรกร
เรื่อง การบริหารจัดการด้านความมั่นคงปลอดภัย

ระเบียบปฏิบัติงาน

๑. ให้มีการทบทวนนโยบายด้านความมั่นคงปลอดภัยอย่างสม่ำเสมอ อย่างน้อย ปีละ ๑ ครั้ง

๒. แสดงเจตนารมณ์ หรือสื่อสารให้เจ้าหน้าที่ทั้งหมด ได้เห็นถึงความสำคัญของการปฏิบัติงานตามนโยบายด้านความมั่นคงปลอดภัยขององค์กรโดยเคร่งครัดอย่างสม่ำเสมอ

๓. ให้มีการสร้างความตระหนักทางด้านความมั่นคงปลอดภัยสารสนเทศเพื่อให้เจ้าหน้าที่ขององค์กรมีความรู้ความเข้าใจ และสามารถป้องกันตนเองได้ในเบื้องต้น อย่างน้อยปีละ ๑ ครั้ง

๔. ให้มีการประเมินความเสี่ยงสำหรับเทคโนโลยีสารสนเทศ ปีละ ๑ ครั้ง

๕. ทำแผนบริหารความเสี่ยงจากปัญหาที่พบ และป้องกันปัญหาที่จะเกิดขึ้นในอนาคต เพื่อลดความเสี่ยง

๖. ให้มีการตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ โดยผู้ตรวจสอบภายในด้านสารสนเทศ ไม่น้อยกว่าปีละ ๑ ครั้ง และให้มีการจัดทำแผนเพื่อปรับปรุง หรือแก้ไขปัญหาที่พบ

๗. ให้มีการแจ้งเวียนให้เจ้าหน้าที่ทั้งหมดขององค์กรได้ระมัดระวัง และดูแลทรัพย์สินขององค์กรที่ตนเองใช้งาน เพื่อป้องกันการสูญหายอย่างน้อยปีละ ๑ ครั้ง

๘. กำหนดนโยบายการใช้งานระบบเครือข่ายอย่างชัดเจนว่า บริการใดที่อนุญาตให้ใช้งานและบริการใดไม่อนุญาต

๙. ห้ามเข้าเว็บไซต์ที่อยู่ในประเภทดังต่อไปนี้

- วิพากษ์วิจารณ์ที่เกี่ยวข้องกับ ชาติ ศาสนา และ พระมหากษัตริย์
- การพนัน
- ลามก อนาจาร
- อื่น ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ผิดศีลธรรม หรือผิดจริยธรรม
- งดเว้นการเล่นเกมส์ ดูภาพยนตร์ หรือฟังเพลง ผ่านทางอินเทอร์เน็ตในเวลาทำงาน

ระเบียบปฏิบัติงาน
เรื่อง การจัดการกับเอกสารที่เกี่ยวข้องกับระบบ

ระเบียบปฏิบัติ

๑. ปรับปรุงคู่มือการปฏิบัติงานให้มีความทันสมัย รวมทั้งให้จัดเก็บไว้ในสถานที่มีความปลอดภัย อย่างน้อยให้ครอบคลุมระบบงาน เครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์ที่มีความสำคัญ ดังนี้

- คู่มือการระบบงานต่าง ๆ ทั้งในส่วนของผู้ใช้งาน และผู้ดูแลระบบ
- คู่มือการตรวจสอบสถานะของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่าย
- คู่มือการตรวจสอบระบบและอุปกรณ์ต่าง ๆ ในห้องเครื่อง
- คู่มือการสำรองข้อมูล

๒. หากมีการจัดเก็บคู่มือการปฏิบัติงานไว้บนระบบเครือข่าย จัดให้มีการป้องกันการเข้าถึง เพื่อให้เฉพาะผู้ที่เกี่ยวข้องเท่านั้น

ระเบียบปฏิบัติงาน
เรื่อง การจัดการระบบเครือข่าย

ระเบียบปฏิบัติ

๑. ปรับปรุงผังเครือข่ายองค์การตลาดเพื่อเกษตรกรให้มีความทันสมัยอย่างน้อยปีละ ๑ ครั้ง

๒. จัดแบ่ง และปรับปรุงระบบเครือข่ายออกเป็นกลุ่มๆ ตามลักษณะการใช้งาน เช่น แบ่งตามกลุ่มเครื่องคอมพิวเตอร์แม่ข่าย (Server) เครื่องลูกข่าย (Client) และ ระบบงานที่สำคัญ

๓. จำกัดการเชื่อมต่อไปยังเครื่องเครื่องคอมพิวเตอร์แม่ข่าย (Server) ระบบงาน หรืออุปกรณ์ที่มีความสำคัญ โดยกำหนดให้เครื่องคอมพิวเตอร์ที่สามารถเชื่อมต่อได้ต้องเป็นเครื่องที่มาจากเครื่องของผู้ดูแลระบบเท่านั้น

๔. กำหนดให้ใช้โปรแกรมมาตรฐานที่มีการเข้ารหัสข้อมูลที่ใช้สำหรับการเชื่อมต่อจากภายในเครือข่ายเพื่อเข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server) หรืออุปกรณ์เครือข่าย

๕. กำหนดให้ใช้โปรแกรมมาตรฐานที่มีการเข้ารหัสข้อมูลที่ใช้สำหรับการเชื่อมต่อจากระยะไกลภายนอกองค์กรเข้ามาสู่เครือข่ายภายในองค์กร

๖. ติดตั้ง Patch แบบอัตโนมัติ บนเครื่องคอมพิวเตอร์ส่วนบุคคลของผู้ใช้งาน

๗. ห้ามติดตั้งเครือข่ายที่ไม่ผ่านระบบความปลอดภัยจากกองเทคโนโลยีและสารสนเทศก่อนได้รับอนุญาต

ระเบียบปฏิบัติงาน
เรื่อง การใช้งานห้องคอมพิวเตอร์แม่ข่าย (Server)

ระเบียบปฏิบัติ

๑. ห้ามนำบุคคลภายนอกเข้าไปในห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) โดยไม่มีกิจจำเป็น

๒. ห้ามนำอาหารและเครื่องดื่มเข้าไปในบริเวณห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๓. ตรวจสอบประตูทางเข้า ออก และหน้าต่างของห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) ให้ปิดล็อคอยู่เสมอ

๔. ตรวจสอบสภาพการทำงานของอุปกรณ์สนับสนุนการทำงานของระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server) ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ ได้แก่

- ระบบกระแสไฟฟ้า
- ระบบการระบายอากาศ
- ระบบการปรับอุณหภูมิ
- ระบบ UPS

๕. จัดวางเครื่องคอมพิวเตอร์ อุปกรณ์สื่อสาร หรือทรัพย์สินอื่นๆ ไว้ในบริเวณที่มีความปลอดภัย ระมัดระวังการจัดตั้งอุปกรณ์ให้อยู่ในสภาพที่มั่นคงและไม่ล้มหรือโอนเอียงได้โดยง่าย

๖. ตรวจสอบการทำงานของอุปกรณ์ดับเพลิงอย่างน้อยปีละ ๑ ครั้ง ว่ายังใช้งานได้เป็นปกติหรือไม่

๗. ให้ดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของเครื่องคอมพิวเตอร์แม่ข่าย (Server) อย่าง สม่ำเสมอ ต้องไม่เก็บกล่องกระดาษ หรือสิ่งที่จะเป็นเชื้อเพลิงไว้ในห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๘. ตรวจสอบและจัดเก็บสัญญาณสื่อสารให้อยู่ในสภาพเป็นระเบียบเรียบร้อย

๙. ดำเนินการจัดทำหรือต่อสัญญาการบำรุงรักษาระบบงาน ไฟร์วอลล์ (Firewall) เราท์เตอร์ (Router) อุปกรณ์สำรองไฟฟ้า (UPS) สำหรับระบบงานสำคัญ และเครื่องปรับอากาศในห้องคอมพิวเตอร์แม่ข่าย ให้ครบถ้วน

๑๐.จัดให้ระบบงานสำคัญ เครื่องเซิร์ฟเวอร์ และอุปกรณ์ที่มีความสำคัญต้อง มีอุปกรณ์สำรองไฟฟ้า (UPS) และ ระบบไฟฟ้าสำรอง เพื่อสนับสนุนการทำงานอย่างครบถ้วน

ระเบียบปฏิบัติงาน
เรื่อง การจัดการทรัพยากรของเครื่องเซิร์ฟเวอร์ (Server)

ระเบียบปฏิบัติ

๑. ดำเนินการตรวจสอบทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย (Server) สำหรับระบบงานสำคัญ อย่างน้อยเดือนละ ๑ ครั้ง สิ่งที่ควรตรวจสอบ ประกอบด้วย ปริมาณการใช้ CPU ปริมาณการใช้ฮาร์ดดิสก์ ปริมาณการใช้หน่วยความจำ และปริมาณการใช้เครือข่าย รวมทั้ง ควรมีการตรวจสอบการใช้งานเครือข่าย

๒. บันทึกข้อมูลการใช้ทรัพยากรดังกล่าวไว้ เพื่อใช้ในการตรวจสอบแนวโน้มการใช้ทรัพยากร รวมทั้งวางแผนจัดซื้อเพิ่มเติมตามความจำเป็นในอนาคต

ระเบียบปฏิบัติงาน
เรื่อง การจัดการไวรัสคอมพิวเตอร์

ระเบียบปฏิบัติ

๑. ตรวจสอบว่าเครื่องคอมพิวเตอร์แม่ข่าย (Server) สำหรับป้องกันไวรัสคอมพิวเตอร์ (Antivirus Server) ยังทำงานตามปกติ และมีการปรับปรุงฐานข้อมูลไวรัส โดยทำการตรวจสอบอย่างน้อยวันละ ๑ ครั้ง หากพบว่าทำงานผิดปกติให้รีบดำเนินการแก้ไข

๒. ทำการติดตั้งโปรแกรมป้องกันไวรัสให้กับผู้ใช้งาน

๓. ทำการติดตั้งและปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยกับเครื่องลูกข่ายทั้งหมด เครื่องคอมพิวเตอร์แม่ข่าย (Server) สำหรับระบบงาน

ระเบียบปฏิบัติงาน
เรื่อง การสำรองข้อมูล

ระเบียบปฏิบัติ

๑. กำหนดรายชื่อของระบบงานสำคัญทั้งหมด

๒. กำหนดผู้รับผิดชอบในการสำรองข้อมูล

๓. กำหนดชนิดของข้อมูลบนระบบงานหรือบน เครื่องคอมพิวเตอร์แม่ข่าย (Server) ดังกล่าว ที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้อย่างน้อยประกอบด้วย

- ข้อมูลในฐานข้อมูลระบบงาน
- ข้อมูลสำหรับตัวระบบ เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง

๔. กำหนดความถี่ในการสำรองข้อมูลของระบบงานหรือเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๕. ทำการสำรองข้อมูลตามความถี่กำหนดไว้ และควรนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่ อย่างน้อย ๑ ชุด

ระเบียบปฏิบัติงาน
เรื่อง การลงทะเบียนและควบคุมการเข้าถึงระบบ

ระเบียบปฏิบัติ

๑. กำหนดให้มีการลงทะเบียนสำหรับผู้ใช้งานใหม่ตาม “แบบฟอร์มสำหรับลงทะเบียนผู้ใช้งาน” และกำหนดสิทธิของผู้ใช้งานตามที่ระบุไว้ในแบบฟอร์มฯ แต่ควรให้สิทธิตามความจำเป็นในการใช้งานเท่านั้น

๒. ให้ทบทวนบัญชีผู้ใช้งานและสิทธิของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง

๓. ดำเนินการจัดส่งบัญชีผู้ใช้งานและรหัสผ่าน และส่งไปยังผู้ใช้งาน

ระเบียบปฏิบัติงาน
เรื่อง การพัฒนาระบบงาน

ระเบียบปฏิบัติ

๑. จัดให้มีการตรวจรับและทดสอบระบบงานใหม่ โดยผู้ใช้งานที่เกี่ยวข้อง ให้ครอบคลุมตามข้อกำหนดที่ ระบุ จนกระทั่ง สามารถใช้งานได้ตรงตามความต้องการของหน่วยงาน จึงจะเปิดให้บริการระบบงานนั้น

๒. สำหรับระบบงานสำคัญ ให้กำหนดมาตรฐานการเข้ารหัสข้อมูลที่มีการรับ – ส่งระหว่างเครื่องลูกข่าย กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และกำหนดให้พัฒนาระบบตามมาตรฐาน

๓. ตรวจสอบข้อมูลตามแนวทางก่อนนำเข้าระบบงาน

๔. ทำการทดสอบระบบงาน และบันทึกผลการทดสอบเก็บไว้เป็นลายลักษณ์อักษร ตามแนวทางการตรวจสอบข้อมูลนำเข้า

๕. พัฒนาระบบงานเพื่อให้สามารถกำหนดรหัสผ่านที่มีความเข้มแข็งตามระเบียบปฏิบัติสำหรับการตั้ง รหัสผ่าน และกำหนดให้รหัสผ่านมีอายุการใช้งาน ๙๐ วัน เมื่อใช้งานครบกำหนดจะต้องทำการกำหนดรหัสผ่าน ใหม่ เพื่อเข้าใช้งานระบบต่อไป

๖. รวบรวมและจัดเก็บซอร์สโค้ดของระบบงานทั้งหมดไว้ในสถานที่เดียวกันที่มีความปลอดภัย และควบคุมให้มีเวอร์ชันของซอร์สโค้ด อย่างน้อย ๒ เวอร์ชันล่าสุด และกำหนดให้ผู้ที่เกี่ยวข้องเท่านั้น ที่สามารถเข้าถึงได้

๗. จัดให้มีการอบรมการใช้งานระบบงานใหม่ให้แก่ผู้ใช้งานทั้งหมดที่เกี่ยวข้อง

๘. จัดทำคู่มือการใช้งานสำหรับระบบงานใหม่ อย่างน้อยสำหรับผู้ใช้งาน และผู้ดูแลระบบ

ระเบียบปฏิบัติงาน
เรื่อง การใช้งานคอมพิวเตอร์และระบบเครือข่าย

ระเบียบปฏิบัติ

๑. กฎระเบียบการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย

๑.๑ เครื่องคอมพิวเตอร์และระบบเครือข่ายขององค์การตลาดเพื่อเกษตรกร เป็นสมบัติของทางราชการ ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต

๑.๒ ผู้ใช้งานต้องยอมรับอย่างไม่มีเงื่อนไขในการรับทราบกฎระเบียบหรือนโยบายต่าง ๆ ที่กำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบายของส่วนราชการ มิได้

๑.๓ บัญชีผู้ใช้งาน (User Account) องค์การตลาดเพื่อเกษตรกร เป็นการให้สิทธิ์เฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน จำหน่าย หรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

๑.๔ บัญชีผู้ใช้งาน (User Account) ที่องค์การตลาดเพื่อเกษตรกร ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดขึ้น รวมถึง ผลเสียหายต่าง ๆ ที่เกิดจาก บัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่ จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๑.๕ ห้ามผู้ใช้งานปฏิบัติการใด ๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมาย หรือศีลธรรม อันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบขององค์การตลาดเพื่อเกษตรกร

๑.๖ ห้ามผู้ใช้งานทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้า หรือการแสวงหาผลกำไรผ่านเครื่อง คอมพิวเตอร์และ ระบบเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไป ซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่ บุคคลทั่วไปเพื่อแสวงหากำไร

๑.๗ ห้ามเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงโดยไม่ได้รับอนุญาต

๑.๘ กรณีเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงเกิดชำรุดเสียหาย ห้ามดำเนินการแก้ไขหรือเปลี่ยนอุปกรณ์ด้วยตนเองเด็ดขาด ให้รีบแจ้งเจ้าหน้าที่กองเทคโนโลยีและสารสนเทศเพื่อดำเนินการแก้ไข

๑.๙ ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น กล่าวคือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลง หรือ แก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (hack) เข้าสู่บัญชีผู้ใช้งาน (user account) ของ ผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ของหน่วยงาน หน่วยงานอื่นๆ การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความ เสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือ

๑.๑๐ ผู้ใช้งานสัญญาว่าจะปฏิบัติตามเงื่อนไข/กฎ/ระเบียบ/คำแนะนำที่องค์การตลาดเพื่อเกษตรกร กำหนดไว้ และ และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสม ซึ่งจะมีผลบังคับใช้โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า

๑.๑๑ องค์การตลาดเพื่อเกษตรกรทรงไว้ซึ่งสิทธิที่จะปฏิเสธการ เชื่อมต่อ และ/หรือการใช้งานและทรงไว้ซึ่งสิทธิที่จะยกเลิก หรือระงับการเชื่อมต่อ และ/หรือการใช้งานใด ๆ ของ ผู้ใช้งานที่ล่วงละเมิด หรือพยายามจะล่วงละเมิดกฎระเบียบนี้ ของส่วนราชการ

๒. กฎระเบียบการเชื่อมต่อเครื่องคอมพิวเตอร์และระบบเครือข่าย

๒.๑ ต้องการนำอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ ต้องปฏิบัติตามกฎระเบียบ ข้อกำหนดโดยเคร่งครัด เพื่อให้การเชื่อมต่ออุปกรณ์ต่าง ๆ เป็นไปตามมาตรฐานสากล และไม่เกิดผลกระทบกับ ระบบเครือข่ายคอมพิวเตอร์ส่วนรวมขององค์กร การขออนุญาตใช้งานเครือข่ายย่อยหมายเลขไอพี (Subnet) ของ หน่วยงานใด ๆ หน่วยงานนั้นจะต้องติดต่อขออนุญาตมายังกองเทคโนโลยีและสารสนเทศ เพื่อพิจารณาดำเนินการ

๒.๒ ไม่อนุญาตให้บุคคลใดกระทำการเคลื่อนย้าย หรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลางโดยพลการ เพราะอาจก่อให้เกิดความเสียหายแก่อุปกรณ์ส่วนกลางและระบบเครือข่ายขององค์การตลาดเพื่อเกษตรกรได้

ระเบียบปฏิบัติงาน
เรื่อง การป้องกันไวรัส

ระเบียบปฏิบัติ

๑. ตรวจสอบว่าโปรแกรมป้องกันไวรัส (Anti Virus) คอมพิวเตอร์ ยังทำงานตามปกติ และมีการปรับปรุงฐานข้อมูลไวรัส (Virus Definition) หรือไม่ โดยตรวจสอบอย่างน้อยวันละ ๑ ครั้ง หากพบว่าทำงานผิดปกติ ให้รีบแจ้งเจ้าหน้าที่กองเทคโนโลยีและสารสนเทศเพื่อดำเนินการแก้ไขโดยทันที

๒. หากเครื่องคอมพิวเตอร์ของผู้ใช้งานยังไม่มีโปรแกรมตรวจสอบไวรัส หรือพบ Virus กรณีพบ Virus แต่ โปรแกรมป้องกันไวรัส ไม่สามารถกำจัดได้ ให้รีบแจ้งกองเทคโนโลยีและสารสนเทศทันที

ระเบียบปฏิบัติงาน
เรื่อง การใช้งานคอมพิวเตอร์และอินเทอร์เน็ต

ระเบียบปฏิบัติ

๑. กฎระเบียบการใช้งานอินเตอร์เน็ต

๑.๑ เครื่องคอมพิวเตอร์และเครือข่ายขององค์การตลาดเพื่อเกษตรกร ได้เป็นสมบัติของทางราชการ ห้ามผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต

๑.๒ ผู้ใช้งานต้องยอมรับอย่างไม่มีเงื่อนไขในการรับทราบกฎระเบียบหรือนโยบายต่าง ๆ ที่กำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบายของส่วนราชการมิได้

๑.๓ บัญชีผู้ใช้งาน (User Account) ขององค์การตลาดเพื่อเกษตรกร เป็นการให้สิทธิ์เฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนจำหน่าย หรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

๑.๔ บัญชีผู้ใช้งาน (User Account) ที่องค์การตลาดเพื่อเกษตรกร ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้น รวมถึง ผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๑.๕ ห้ามผู้ใช้งานปฏิบัติการใด ๆ เกี่ยวกับข้อมูลข่าวสารที่เป็นการขัดต่อกฎหมาย หรือศีลธรรม อันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบขององค์การตลาดเพื่อเกษตรกร

๑.๖ ห้ามผู้ใช้งานทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้า หรือการแสวงหาผลกำไรผ่านอินเตอร์เน็ต เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการ ค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำาไร

๑.๗ ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่นกล่าว คือ ผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือ แก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (hack) เข้าสู่บัญชีผู้ใช้งาน (user account) ของ ผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ของหน่วยงาน หรือหน่วยงานอื่นๆ การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความ เสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการ ละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว องค์การตลาดเพื่อเกษตรกรไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๑.๘ องค์การตลาดเพื่อเกษตรกรจะไม่ควบคุมเนื้อหาของข้อมูล ข่าวสารที่เก็บ และรับ-ส่งผ่านเข้าออกเครื่องคอมพิวเตอร์ของหน่วยงาน และจะไม่รับประกันในคุณภาพของการ เก็บการรับ-ส่งข้อมูล ข่าวสาร และการไม่สามารถใช้งานได้ของระบบบางส่วนหรือทั้งหมด และจะไม่รับผิดชอบใน ความเสียหายของการใช้งานอันเนื่องมาจาก วงจรสื่อสารชำรุด จานแม่เหล็กชำรุด ความล่าช้า แฟ้มข้อมูลหรือ จดหมายส่งไปไม่ถึงปลายทาง หรือส่งผิดสถานที่ และความผิดพลาดในข้อมูลหรือความเสียหายอันเกิดจากการล่วง ละเมิดโดยผู้ใช้งาน อื่นๆ

๑.๙ ผู้ใช้งานสัญญาว่าจะปฏิบัติตาม เงื่อนไข/กฎ/ระเบียบ/คำแนะนำที่องค์การตลาดเพื่อเกษตรกรกำหนดไว้และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสม ซึ่งจะมีผลบังคับใช้โดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า

๑.๑๐ องค์การตลาดเพื่อเกษตรกร ทรงไว้ซึ่งสิทธิที่จะปฏิเสธการ เชื่อมต่อ และ/หรือการใช้งาน และทรงไว้ซึ่งสิทธิที่จะยกเลิก หรือระงับการเชื่อมต่อ และ/หรือการใช้งานใดๆ ของ ผู้ใช้งานที่ล่วงละเมิด หรือพยายามจะล่วงละเมิดกฎระเบียบนี้ของส่วนราชการ

ระเบียบปฏิบัติงาน
เรื่อง การใช้งานอีเมล์

ระเบียบปฏิบัติ

๑. ห้ามมิให้เข้าถึงข้อมูลอีเมล์ของบุคคลอื่นโดยไม่ได้รับอนุญาต
๒. ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)
๓. ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)
๔. ห้ามส่งอีเมล์ที่มีลักษณะเป็นการละเมิดต่อกฎหมาย หรือสิทธิของบุคคลอื่น
๕. ห้ามส่งอีเมล์ที่มีไวรัสคอมพิวเตอร์ไปให้กับบุคคลอื่นโดยเจตน
๖. ห้ามปลอมแปลงอีเมล์ของบุคคลอื่น
๗. ห้ามรับ หรือส่งอีเมล์แทนบุคคลอื่น โดยไม่ได้รับอนุญาต
๘. ห้ามส่งอีเมล์ที่เป็นความลับขององค์กร เว้นแต่ใช้วิธีการเข้ารหัสข้อมูลอีเมล์ที่องค์กรกำหนดไว้
๙. ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่อีเมล์ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัว
๑๐. ให้ใช้ความระมัดระวังในการจำกัดกลุ่มผู้รับอีเมล์เท่าที่มีความจำเป็นต้องรับรู้รับทราบในข้อมูลที่ส่งไป
๑๑. ให้ใช้คำที่สุภาพในการส่งอีเมล์
๑๒. ให้ระบุชื่อของผู้ส่งในอีเมล์ทุกฉบับที่ส่งไป
๑๓. ให้ทำการสำรองข้อมูลอีเมล์ตามความจำเป็น

ระเบียบปฏิบัติงาน
เรื่อง การป้องกันการใช้ทรัพยากรผิดวัตถุประสงค์

ระเบียบปฏิบัติ

๑. เพื่อป้องกันการกระทำผิดกฎหมาย หรือเพื่อป้องกันการก่อให้เกิดความเสียหายแก่บุคคลอื่น

๒. เพื่อป้องกันการกระทำที่ขัดต่อ พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๓. เพื่อป้องกันการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๔. เพื่อป้องกันการค้าขาย หรือผลประโยชน์ส่วนตัว หรือผลประโยชน์ทางการเมือง

๕. เพื่อป้องกันการเข้าถึง แสดง จัดเก็บ แจกจ่าย แก้ไข จัดทำ หรือบันทึกข้อมูลที่มีเนื้อหาไม่เหมาะสม เช่น ข้อมูลอันเป็นเท็จ ข้อมูลที่มีผลต่อความมั่นคงของสถาบันชาติ ศาสนาและพระมหากษัตริย์ ภาพลามก อนาจาร ภาพตัดต่อของบุคคลอื่น หรือข้อมูลที่ก่อให้เกิดความ เสื่อมเสียอับอายแก่องค์กรหรือบุคคลอื่น เป็นต้น

๖. เพื่อป้องกันการเผยแพร่ข้อมูล หรืออนุญาตให้ผู้อื่นเผยแพร่ข้อมูลเพื่อการกล่าวร้าย หมิ่นประมาทหรือพาดพิง บุคคลอื่น จนทำให้องค์กรถูกฟ้องร้องหรือก่อให้เกิดความเสียหายแก่องค์กร

๗. เพื่อป้องกันการเปิดเผยข้อมูลลับซึ่งได้มาจากการปฏิบัติงานให้แก่องค์กรไม่ว่าจะเป็นข้อมูลขององค์กรหรือบุคคลภายนอกก็ตาม

๘. เพื่อป้องกันขัดขวางหรือโจมตี การใช้งานระบบเครือข่ายขององค์กร หรือของหน่วยงานภายนอกอื่น

๙. เพื่อป้องกันการแพร่กระจายไวรัส หนอน ม้าโทรจัน สปายแวร์ สแปมเมล์ หรือโปรแกรมไม่ประสงค์อื่นๆ

๑๐. เพื่อป้องกันอาจขัดต่อผลประโยชน์ขององค์กร หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายต่อองค์กร

ระเบียบปฏิบัติงาน
เรื่อง การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

ระเบียบปฏิบัติ

๑. ในกรณีที่เป็นเครื่องคอมพิวเตอร์แบบพกพาที่ใช้ร่วมกัน ให้กรอกแบบฟอร์มยืม - คืนสำหรับเครื่องคอมพิวเตอร์แบบพกพานั้น เพื่อขออนุมัติการนำไปใช้งาน และป้องกันการสูญหาย

๒. ตรวจสอบอย่างสม่ำเสมอว่า โปรแกรมป้องกันไวรัสที่ใช้งานอยู่ ได้รับการปรับปรุงฐานข้อมูลรูปแบบไวรัสอย่างสม่ำเสมอ

๓. ให้ระมัดระวังและรักษาเครื่องคอมพิวเตอร์แบบพกพา เมื่อมีการนำไปใช้งานนอกสถานที่เพื่อป้องกันการสูญหาย หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔. เมื่ออยู่ในที่สาธารณะหรือในห้องประชุม ห้ามปล่อยเครื่องคอมพิวเตอร์ทิ้งไว้โดยไม่มีผู้ดูแล

๕. ตรวจสอบว่าได้มีการตั้งค่าโปรแกรมพักหน้าจอ (Screen Saver) เพื่อให้ทำการล็อกหน้าจอ โดยอัตโนมัติ หลังจากที่ไม่ได้ใช้งานเกินกว่า ๑๕ นาที

ระเบียบปฏิบัติงาน
เรื่อง สำหรับการตั้งรหัสผ่าน กำหนดและป้องกัน

ระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน

๑. มีความยาวไม่น้อยกว่า ๘ ตัวอักษร ยกเว้นระบบเก่า ๆ ที่ไม่สามารถดำเนินการได้

๒. มีการผสมผสานกันระหว่างตัวอักษรที่เป็นตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

๓. ไม่กำหนดรหัสผ่านจากคำศัพท์ที่ปรากฏในพจนานุกรม

๔. เปลี่ยนรหัสผ่านทุกๆ ๓ เดือน สำหรับเจ้าหน้าที่ทั่วไปและสำหรับเจ้าหน้าที่ของกองเทคโนโลยีและสารสนเทศ

ระเบียบปฏิบัติสำหรับการกำหนดและป้องกันรหัสผ่าน

๑. เก็บรักษารหัสผ่านของตนเองไว้เป็นความลับ ห้ามเปิดเผยต่อผู้อื่น

๒. กำหนดรหัสผ่านให้มีคุณสมบัติ ตามระเบียบปฏิบัติสำหรับการตั้งรหัสผ่าน

๓. กำหนดรหัสผ่านสำหรับการใช้ไฟล์ข้อมูลร่วมกันบนเครือข่าย

๔. ห้ามบันทึกรหัสผ่านไว้ในโปรแกรม คอมพิวเตอร์เพื่อช่วยในการจำรหัสผ่านของตน (เช่น ในโปรแกรมเว็บบราวเซอร์จะสามารถเลือกให้โปรแกรมช่วยจำรหัสผ่านไว้ให้)

๕. ต้องไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นโดยบุคคลอื่น

๖. ในกรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ ผู้อื่นเพื่อให้สามารถปฏิบัติงานแทนตนเองได้ หลังจากที่ทำงานนั้นเสร็จเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

ระเบียบปฏิบัติงาน
เรื่อง การนำข้อมูลเผยแพร่สู่สาธารณะ

ระเบียบปฏิบัติ

๑. ให้ผู้ที่เป็นเจ้าของข้อมูลที่ต้องการนำข้อมูลนั้นขึ้นเผยแพร่สู่สาธารณะ เช่น การเผยแพร่ผ่านทางเว็บไซต์ขององค์การตลาดเพื่อเกษตรกร จะต้องทำการตรวจสอบ ความถูกต้องของข้อมูลก่อน หากมีความผิดพลาดเกิดขึ้นกับเนื้อหาจะต้องรับผิดชอบต่อความผิดพลาดนั้น

๒. ให้ผู้ที่มีหน้าที่รับผิดชอบในการนำข้อมูลขึ้นเผยแพร่สู่สาธารณะ เช่น การเผยแพร่ผ่านทางเว็บไซด์ขององค์การตลาดเพื่อเกษตรกร จะต้องดำเนินการด้วยตนเอง โดย ห้ามมิให้ผู้อื่น ดำเนินการแทน