ประกาศสำนักเลขาธิการนายกรัฐมนตรี
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๕๔

เพื่อให้การใช้งานสารสนเทศทางอิเล็กทรอนิกส์ของสำนักเลขาธิการนายกรัฐมนตรี มีความมั่นคงปลอดภัยอย่างเหมาะสมและมีประสิทธิภาพ รวมทั้งเพื่อเป็นการป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง อันเป็นเหตุให้เกิดภัยคุกคามต่างๆ ที่ก่อให้เกิดความเสียหายหรือเสื่อมเสียแก่สำนักเลขาธิการนายกรัฐมนตรี และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้อง สำนักเลขาธิการนายกรัฐมนตรี จึงเห็นสมควรให้กำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรีขึ้น โดยมีวัตถุประสงค์และองค์ประกอบของนโยบาย ดังต่อไปนี้

๑. <u>วัตถุประสงค์</u>

๑.๑ เพื่อกำหนดแนวนโยบายและแนวปฏิบัติให้ผู้บริหาร ผู้ปฏิบัติงาน ผู้ดูแลระบบ และบุคคลภายนอกที่มาปฏิบัติงานให้กับสำนักเลขาธิการนายกรัฐมนตรี ใช้ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างมีประสิทธิภาพ

๑.๒ เพื่อกำหนดขอบเขตการบริหารจัดการ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี ให้มีความสอดคล้องกับมาตรฐาน ISO/IEC 27001 และมีการติดตามปรับปรุงให้ทันสมัยอย่างต่อเนื่อง

๑.๓ เพื่อส่งเสริมให้มีการเผยแพร่ นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี แก่ผู้ใช้ในทุกระดับได้รับทราบอย่างทั่วถึง และยอมรับที่จะปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

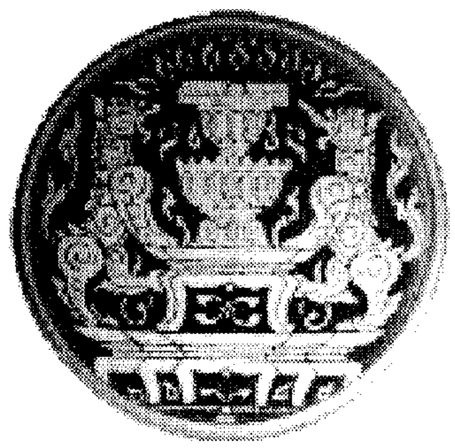
๒. <u>องค์ประกอบของนโยบาย</u>

องค์ประกอบของนโยบาย จะใช้แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการนายกรัฐมนตรี ปี พ.ศ.๒๕๕๔ ปรากฏตาม แนบท้ายประกาศนี้

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ ผู้ใช้ที่ได้รับสิทธิเข้าใช้งานสารสนเทศทางอิเล็กทรอนิกส์ของสำนักเลขาธิการนายกรัฐมนตรี ทุกระดับและทุกกรณี จะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศ ณ วันที่ ๓๐ กันยายน พ.ศ.๒๕๕๔

(นางสาวสมลักษณ์ ส่งสัมพันธ์)
รองเลขาธิการนายกรัฐมนตรีฝ่ายบริหาร
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ประจำสำนักเลขาธิการนายกรัฐมนตรี



แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักเลขาธิการนายกรัฐมนตรี
พ.ศ. ๒๕๕๔

จัดทำโดย

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักเลขาธิการนายกรัฐมนตรี

สารบัญ

คำนำ

ในปัจจุบันปัญหาด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีความรุนแรงเพิ่มขึ้นทั้งในประเทศและต่างประเทศ อีกทั้งมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐมากยิ่งขึ้น หน่วยงานมีความจำเป็นอย่างยิ่งที่จะต้องมีนโยบายการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย ซึ่งต้องมีการควบคุมจัดการด้านความมั่นคงปลอดภัยที่ดีเพื่อให้เกิดความปลอดภัยจากการโจมตี รวมทั้งจะต้องดูแลระบบและโปรแกรมต่าง ๆ ผ่านระบบเครือข่าย ระดับการให้บริการ การจัดการทุกเครือข่ายโดยใช้กรรมวิธีมาตรฐานและอุปกรณ์ที่ได้รับการทดสอบด้านความมั่นคงปลอดภัยตามมาตรฐานสากลการต่อเชื่อมเครือข่าย การดำเนินการใด ๆ ก็ตามจะต้องคำนึงถึงข้อบังคับและกฎหมาย และต้องให้ความสำคัญกับการฝ่าฝืนต่อการรักษาความปลอดภัยของข้อมูล เพื่อให้ผู้ใช้งานระบบและเครือข่ายนำไปปฏิบัติอย่างถูกต้องและมีประสิทธิภาพอย่างแท้จริง

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักเลขาธิการนายกรัฐมนตรี พ.ศ. ๒๕๕๔

๑. หลักการและเหตุผล

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานภาครัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ พ.ศ. ๒๕๕๓ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ สำนักเลขาธิการนายกรัฐมนตรีจึงได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงสารสนเทศ โดยการดำเนินการให้สอดคล้องกับมาตรฐานด้านความมั่นคงปลอดภัยสากลได้แก่มาตรฐาน ISO/IEC 27001 และต้องลดผลกระทบจากภัยคุกคามต่าง ๆ ตลอดจนการฟื้นฟูระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลง รวมทั้งต้องจัดหาเครื่องมือที่จำเป็นอย่างพอเพียงเพื่อที่จะสนับสนุนการปฏิบัติงานตามนโยบายได้อย่างมีประสิทธิภาพ

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดทิศทางการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงานให้เป็นไปตามระเบียบปฏิบัติ ข้อบังคับ และกฎหมายที่เกี่ยวข้อง

๒.๒ เพื่อการกำหนดสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ และอุปกรณ์ในการประมวลผลข้อมูลของผู้ใช้งาน

๒.๓ เพื่อดำเนินการจัดทำระบบสารสนเทศและคัดเลือกระบบสำรองสารสนเทศที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน และการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถใช้งานสารสนเทศได้ตามปกติ

๒.๔ เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๓. แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักเลขาธิการนายกรัฐมนตรี

๓.๑ กำกับดูแลผู้ใช้งานให้ปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด หากมีการละเมิดหรือฝ่าฝืนจะต้องมีบทลงโทษตามความเหมาะสม รวมทั้งต้องหามาตรการหรือแนวทางแก้ไขปัญหาที่มีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้นจากเหตุฉุกเฉิน และต้องติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามระเบียบปฏิบัติ ข้อบังคับ และกฎหมายที่เกี่ยวข้อง

๓.๒ กำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๓.๓ เผยแพร่ความรู้ ความเข้าใจ และการอบรมด้านความมั่นคงปลอดภัยสารสนเทศเพื่อเสริมสร้างความตระหนักให้กับผู้ใช้งานทั้งภายในหน่วยงานและหน่วยงานภายนอกที่เกี่ยวข้อง

๓.๔ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

๔. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักเลขาธิการนายกรัฐมนตรี

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักเลขาธิการนายกรัฐมนตรี จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยกำหนดแนวปฏิบัติดังต่อไปนี้

ส่วนที่ ๑. แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
ส่วนที่ ๒. แนวปฏิบัติการควบคุมการเข้าถึงระบบ
ส่วนที่ ๓. แนวปฏิบัติการสำรองข้อมูล
ส่วนที่ ๔. แนวปฏิบัติการป้องกันโปรแกรมไม่ประสงค์ดี
ส่วนที่ ๕. แนวปฏิบัติการประเมินความเสี่ยง
ส่วนที่ ๖. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
ส่วนที่ ๗. แนวปฏิบัติตามข้อกำหนดทางกฎหมาย

คำนิยาม

คำนิยามที่ใช้ในประกาศนี้ ประกอบด้วย

หน่วยงาน หมายความว่า สำนักเลขาธิการนายกรัฐมนตรี

ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

ความมั่นคงปลอดภัย หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

ระบบแลน (Local Area Network) และ ระบบอินทราเน็ต (Intranet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเทอร์เน็ต (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

เครื่องคอมพิวเตอร์ หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา

ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

ผู้บังคับบัญชา หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักเลขาธิการนายกรัฐมนตรี

ผู้ใช้บริการ หมายความว่า ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างตามสัญญาจ้างในสังกัดหน่วยงาน และให้หมายความรวมถึงข้าราชการการเมือง หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

ผู้ดูแลระบบ (System Administrator) หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่าย

หน่วยงานภายนอก หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หมายความว่า พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

๑) พื้นที่ทำงาน หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ (System Administrator)

๒) พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย หมายความว่า พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์

๓) พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายความว่า พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย

ทรัพย์สิน หมายความว่า ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

จดหมายอิเล็กทรอนิกส์ (e-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

บัญชีผู้ใช้งาน (Account) หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบเครือข่ายของหน่วยงาน

โปรแกรมประสงค์ร้าย (Malware) หมายความว่า โปรแกรมคอมพิวเตอร์ ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

ชื่อเครื่องคอมพิวเตอร์ (Computer Name) หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

สื่อบันทึกพกพา หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk เป็นต้น

ไบออส (BIOS) หมายความว่า ซอฟต์แวร์ขนาดเล็กซึ่งเก็บอยู่ในหน่วยความจำบนเมนบอร์ดของเครื่องคอมพิวเตอร์ ทำหน้าที่ควบคุมขั้นตอนการบู๊ตและการทำงานของอุปกรณ์พื้นฐานต่างๆ ที่ติดตั้งอยู่บนเมนบอร์ด

การตั้งค่าระบบ (Configuration) หมายความว่า ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

เลขที่อยู่ไอพี (IP Address) หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

เลขที่อยู่ไอพีสาธารณะ (Public IP Address) หมายความว่า เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงาน หรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

แบนด์วิดท์ (Bandwidth) หมายความว่า ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับ ส่งข้อมูล

ชื่อผู้ใช้งาน (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

ลงบันทึกเข้า (Login) หมายความว่า กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

ลงบันทึกออก (Logout) หมายความว่า กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

อัพเดท (Update) หมายความว่า ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

ช่องโหว่ (Vulnerability) หมายความว่า ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยขอบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ไฟล์ที่สามารถประมวลผลได้ (Executable file) หมายความว่า ไฟล์โปรแกรมที่สามารถเรียกใช้งานได้ทันที เช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe ในขณะที่ไฟล์ข้อมูลอื่นๆ จะเป็นไฟล์ข้อมูลประกอบ

การเข้ารหัส (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

อุปกรณ์กระจายสัญญาณ (Access Point) หมายความว่า อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

SSID (Service Set Identifier) หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

โดยปริยาย (Default) หมายความว่า ค่าที่เครื่องคอมพิวเตอร์หรือโปรแกรมได้กำหนดไว้ล่วงหน้า และนำไปใช้ได้โดยปริยายหากไม่มีการเปลี่ยนแปลงจากผู้ใช้บริการ

WEP (Wired Equivalent Privacy) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

WPA (Wi-Fi Protected Access) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

Wireless LAN Client หมายความว่า เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลน โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลแทนการใช้สายสัญญาณ โดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะต้องมีทั้งตัวรับและส่งสัญญาณ ซึ่งมีมาตรฐานที่นิยมใช้เรียกว่า IEEE 802.11

MAC Address (Media Access Control Address) หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

ไฟร์วอลล์ (Firewall) หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

VPN (Virtual Private Network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

Web Server หมายความว่า เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บ และมีหน้าที่ให้บริการเว็บเพจต่างๆ

ชื่อโดเมนย่อย (Sub Domain Name) หมายความว่า ส่วนย่อยที่จะช่วยขยายให้ทราบถึงกลุ่มต่าง ๆ ภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ “ที่อยู่เว็บไซต์” แทนก็ได้

อุปกรณ์จัดเส้นทาง (Router) หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

อุปกรณ์กระจายสัญญาณข้อมูล (Switch) หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล

การพิสูจน์ยืนยันตัวตน (Authentication) หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)

แผนผังระบบเครือข่าย (Network Diagram) หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

Command Line หมายความว่า บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความ เพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ

Firewall Log หมายความว่า การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟร์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์ เพื่อตรวจสอบประเภทของการสื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน

DoD 5220.22-M หมายความว่า การลบข้อมูลอย่างสมบูรณ์ซึ่งได้รับการยอมรับและใช้งานกับกระทรวงกลาโหม ประเทศสหรัฐอเมริกา โดยทำให้ไม่สามารถกู้ไฟล์กลับคืนมาได้ ซึ่งทำการลบข้อมูล ๓ รอบ รอบแรกด้วยข้อมูลแบบสุ่ม รอบที่สองด้วยบิตที่ตรงกันข้าม รอบสุดท้ายด้วยข้อมูลไบต์สุ่ม

ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่ตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Log) และรับผิดชอบให้สามารถเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ (Log)

เวลาอ้างอิงสากล (Stratum 0) หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่าย ที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล ในประเทศไทยนั้นเราอ้างอิงกับหน่วยงานมาตรฐาน (เช่น กรมอุทกศาสตร์ กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ)

ส่วนที่ ๑
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ข้อ ๑ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งพื้นที่ใช้งาน โดยแบ่งเป็นส่วน ๆ ดังนี้ พื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย และพื้นที่ใช้งานระบบเครือข่ายไร้สาย ทั้งนี้จะต้องประกาศให้รับทราบทั่วกัน

ข้อ ๒ ให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำหนดสิทธิ์ในการเข้า-ออกพื้นที่ที่ต้องการรักษาความปลอดภัย

ข้อ ๓ ต้องจัดให้มีการควบคุมการเข้า-ออกในบริเวณหรือพื้นที่ที่ต้องการรักษาความปลอดภัย และอนุญาตให้ผ่านเข้า-ออกได้เฉพาะผู้ที่ได้รับอนุญาต

ข้อ ๔ บุคคลภายนอกหรือผู้มาติดต่อจะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับมอบหมาย และจะต้องลงชื่ออนุญาตการเข้า-ออกในแบบฟอร์ม

ข้อ ๕ กรณีที่บุคคลภายนอกหรือผู้ติดต่อนำอุปกรณ์ เช่น คอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่ายเข้าบริเวณพื้นที่รักษาความปลอดภัยจะต้องลงบันทึกในแบบฟอร์มการเข้า-ออกในรายการอุปกรณ์ที่นำเข้ามาให้ถูกต้อง และจะต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

ข้อ ๖ การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อม

๑) ต้องมีอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควัน เครื่องตรวจจับความร้อน เป็นต้น และมีระบบดับเพลิงแบบอัตโนมัติ เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา

๒) ต้องมีระบบไฟฟ้าสำรองป้องกันมิให้คอมพิวเตอร์ได้รับความเสียหายจากความไม่คงที่ของกระแสไฟฟ้า

๓) ต้องมีระบบควบคุมอุณหภูมิและความชื้นที่เหมาะสม โดยการติดตั้งอุณหภูมิเครื่องปรับอากาศและตั้งค่าความชื้นให้เหมาะสมกับคุณลักษณะ (Specification) ของระบบคอมพิวเตอร์

๔) ในกรณีที่มีการยกระดับพื้นของศูนย์คอมพิวเตอร์ เพื่อติดตั้งระบบปรับอากาศ รวมทั้งเดินสายไฟและสายเครือข่ายด้านล่าง ควรติดตั้งระบบเตือนภัยน้ำรั่วบริเวณที่มีท่อน้ำเพื่อป้องกันหรือระงับเหตุน้ำรั่วได้ทันเวลา

๕) จะต้องเตรียมความพร้อมการใช้งานอุปกรณ์กรณีเกิดความไม่สงบของบ้านเมือง

๖) จะต้องมีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอเพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน

๗) จะต้องไม่นำทรัพย์สินของหน่วยงานออกไปข้างนอก เว้นเสียได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา

ส่วนที่ ๒
แนวปฏิบัติการควบคุมการเข้าถึงสารสนเทศ

การควบคุมการเข้าถึงสารสนเทศ

ข้อ ๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้กำหนดสิทธิ์การเข้าใช้งานระบบสารสนเทศของหน่วยงาน ถ้าเป็นบุคคลจากหน่วยงานภายนอกจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมกับผู้ใช้งาน และต้องมีการทบทวนสิทธิ์การเข้าถึงระบบอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) จะต้องบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจสอบความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) จะต้องบันทึกการเข้าถึงระบบ การแก้ไข การเปลี่ยนแปลง การกำหนดสิทธิ์ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

การบริหารจัดการการเข้าถึงระบบสารสนเทศ

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องระบุสิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร ในการใช้งานระบบเทคโนโลยีสารสนเทศ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น และต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) มีหน้าที่บริหารจัดการสิทธิ์ของบุคลากรดังต่อไปนี้

๑) การยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออก พ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒) แจ้งรหัสผ่าน (Password) ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งทางจดหมายอิเล็กทรอนิกส์ (e-mail)

๓) การกำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๔) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร โดยมีการกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลา หรือพ้นจากตำแหน่ง กำหนดสิทธิ์การเข้าถึงระบบได้ถึงระดับใด และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและ การเข้าถึงผ่านระบบงาน

๒) กำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ตัวตนของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลา

๔) การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายอินเทอร์เน็ต จะต้องเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

การควบคุมการใช้งานบัญชีผู้ใช้งาน (Account)

ข้อ ๑ ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้งาน (Account) ต้องเป็นผู้รับผิดชอบในการกระทำใด ๆ ที่เกิดขึ้นจากการใช้บัญชีผู้ใช้งาน (Account) ของเครื่องคอมพิวเตอร์ และระบบเครือข่าย ยกเว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

ข้อ ๒ ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้งาน (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๓ ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้งาน (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

ข้อ ๔ หากการพิสูจน์ตัวตนมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การโดนล็อค หรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งานต้องแจ้งผู้ดูแลระบบ

การควบคุมการใช้รหัสผ่าน (Password)

ข้อ ๑ รหัสผ่าน (Password) ควรมีความยาวไม่น้อยกว่า ๖ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่างๆ

ข้อ ๒ ไม่ควรกำหนดรหัสผ่าน (Password) จากชื่อ หรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์

ข้อ ๓ การเปลี่ยนรหัสผ่าน (Password) เพื่อใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานทุก ๓-๖ เดือน

ข้อ ๔ ผู้ใช้งานจะต้องเก็บรักษารหัสผ่าน (Password) สำหรับการใช้งานเครื่องคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใด ๆ ให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๕ ผู้ใช้งานต้องไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้วอย่างน้อย ๕ รหัสผ่าน

การเข้าถึงระบบปฏิบัติการ

ข้อ ๑ ผู้ใช้งานต้องพิสูจน์ตัวตนทุกครั้งก่อนการเข้าใช้ระบบปฏิบัติการของเครื่องคอมพิวเตอร์

ข้อ ๒ ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนเองในการเข้าใช้ระบบปฏิบัติการของเครื่องคอมพิวเตอร์

ข้อ ๓ ห้ามทำการปรับแต่งไบออส (BIOS) หรือการตั้งค่าระบบ (Configuration) อื่นใดที่อาจส่งผลกระทบต่อระบบการทำงานของคอมพิวเตอร์อันเป็นเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้ตามปกติ

ข้อ ๔ ผู้ใช้งานควรตั้งค่าเวลาพักหน้าจอ (Screen saver) โดยตั้งเวลาอย่างน้อย ๕ นาที

ข้อ ๕ ผู้ใช้งานจะต้องลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

การเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

ข้อ ๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server)

ข้อ ๒ ห้ามผู้ใช้บริการ และบุคคลภายนอกนำเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์มาเชื่อมต่อเข้าระบบเครือข่ายของหน่วยงาน ทั้งนี้ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๓ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อระบบ และผู้ใช้บริการอื่นๆ

ข้อ ๔ ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมการเข้าถึงระบบเครือข่าย ดังต่อไปนี้

๑) การจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒) การจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๓) กำหนดวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้

๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก

๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจะต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

๗) เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

๘) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๙) การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ดูแลระบบ (System Administrator) และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ ๗ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

๑) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง และระบุตัวบุคคลที่เข้าถึงสื่อ และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูล และห้ามไม่ให้ผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่ได้รับมอบหมาย

๒) ให้มีระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกระบบป้องกันการบุกรุกเช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

๓) ตรวจสอบระบบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ และต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๔) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้อง และนำมาใช้ประโยชน์ได้ ผู้ดูแลระบบต้องตั้งเวลาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum ๐) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ข้อ ๘ ลบข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์แม่ข่าย (Server) อย่างถาวรหรือทำลายข้อมูลที่เกี่ยวข้องกับการปฏิบัติงานของหน่วยงานบนเครื่องคอมพิวเตอร์และระบบเครือข่ายเมื่อหมดความจำเป็นในการใช้งาน ด้วยวิธีการตามมาตรฐาน DoD 5220.22-M

ข้อ ๙ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความมั่นคงปลอดภัยสารสนเทศ ดังต่อไปนี้

๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒) การควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๓) การดำเนินการใด ๆ ที่สามารถเข้าสู่ข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

๕) การเข้าใช้งานระบบต้องทำการพิสูจน์ตัวตน

๖) ห้ามไม่ให้ใช้บริการบนระบบอินเทอร์เน็ต (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth)

๗) ห้ามนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น การตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ซึ่งจะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๘) ทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

๙) กระทำการใด ๆ โดยมิชอบเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

๑๐) กระทำการใด ๆ โดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ในระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์

๑๑) การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ของหน่วยงานจะต้องกำหนดโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

การควบคุมการใช้งานอินเทอร์เน็ต

ข้อ ๑ ไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์ และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

ข้อ ๒ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับของหน่วยงานที่ยังไม่ได้ประกาศเป็นทางการผ่านระบบอินเทอร์เน็ต (Internet)

ข้อ ๓ การดาวน์โหลดโปรแกรมใช้งาน การอัพเดท (Update) โปรแกรมต่างๆ จากระบบอินเทอร์เน็ต (Internet) ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์

ข้อ ๔ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ห้ามเปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน

ข้อ ๕ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เสนอความคิดเห็น หรือใช้ข้อความยั่วยุให้ร้ายซึ่งก่อให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน

ข้อ ๖ ภายหลังจากการใช้งานระบบอินเทอร์เน็ต (Internet) ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

การควบคุมการใช้ไฟร์วอลล์ (Firewall)

ข้อ ๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีอำนาจหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์

ข้อ ๒ การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

ข้อ ๓ ทุกเส้นทางที่เชื่อมต่ออินเทอร์เน็ต และบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

ข้อ ๔ ผู้ใช้บริการอินเทอร์เน็ตจะต้องทำการ Login account ก่อนการใช้งานทุกครั้ง

ข้อ ๕ ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

ข้อ ๖ การเข้าถึงอุปกรณ์ไฟร์วอลล์ เฉพาะผู้ที่ได้รับมอบหมาย

ข้อ ๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้า-ออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๘ การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารอนุญาตให้ ใช้งาน ซึ่ง

หากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นเท่านั้น

ข้อ ๑๐ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๑๑ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณี

ข้อ ๑๒ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มี ความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๓ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๑๔ ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

การควบคุมการใช้เครือข่ายไร้สาย (Wireless)

ข้อ ๑ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) จากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) จะต้องทำการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) กำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

ข้อ ๗ ผู้ดูแลระบบ (System Administrator) จะต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๆ ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งาน

ระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบ (System Administrator) รายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ข้อ ๘ ผู้ดูแลระบบ (System Administrator) ต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในของหน่วยงาน

การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (e-mail)

ข้อ ๑ การลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) โดยการยื่นคำขอกับเจ้าหน้าที่ที่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศมอบหมาย และทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail)

ข้อ ๒ ผู้ใช้งานที่ได้รับรหัสผ่าน (Password) ในการเข้าใช้ระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกควรเปลี่ยนรหัสผ่าน (Password) โดยทันที

ข้อ ๓ ไม่ควรบันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

ข้อ ๔ ทำการเปลี่ยนรหัสผ่าน (Password) ทุก ๆ ๓-๖ เดือน

ข้อ ๕ ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากผู้ใช้งาน และให้ถือว่าผู้ใช้งานเป็นเจ้าของจดหมายอิเล็กทรอนิกส์ (e-mail) ถ้าหากว่าข้อความในจดหมายอิเล็กทรอนิกส์ผิดต่อกฎหมายหรือศีลธรรม ผู้ใช้งานต้องเป็นผู้รับผิดชอบต่อการกระทำ

ข้อ ๖ ภายหลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) จะต้องลงบันทึกออก (Logout) ทุกครั้ง

ข้อ ๗ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงานให้เหมาะสมกับผู้ใช้บริการ และหน้าที่ความรับผิดชอบของผู้ใช้บริการ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การพ้นจากตำแหน่ง หรือการยกเลิกการใช้งาน เป็นต้น

ข้อ ๘ ผู้ดูแลระบบ (System Administrator) จะต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้บริการใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

ส่วนที่ ๓
แนวปฏิบัติการสำรองข้อมูล

ข้อ ๑ จัดทำสำเนาข้อมูล โปรแกรมระบบปฏิบัติการ (Operating System) โปรแกรมระบบงานคอมพิวเตอร์ (Application System) และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน สามารถพร้อมใช้งานได้อย่างต่อเนื่อง โดยการจัดเก็บเป็นหมวดหมู่ ตามระดับชั้นความลับ ข้อกำหนดทางกฎหมาย และระดับความสำคัญของหน่วยงาน

ข้อ ๒ กำหนดขั้นตอนหรือวิธีปฏิบัติการสำรองข้อมูล เพื่อเป็นเป็นแนวทางให้แก่ผู้ปฏิบัติงานโดยมีรายละเอียด ดังนี้

๑) ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง

๒) ประเภทสื่อบันทึก (media)

๓) จำนวนที่ต้องสำรอง (copy)

๔) วิธีการเก็บรักษาสื่อบันทึก

๕) จัดทำป้ายชื่อระบุชื่อซอฟต์แวร์ วันที่ เวลา ที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

ข้อ ๓ การขอใช้งานสื่อบันทึกข้อมูลสำรองควรได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมาย และควรจัดทำทะเบียนคุมการรับและส่งมอบสื่อบันทึกข้อมูลสำรอง โดยต้องระบุผู้รับ ผู้ส่ง ผู้อนุมัติ ประเภทข้อมูล และเวลาอย่างชัดเจน

ข้อ ๔ ควรมีขั้นตอนหรือวิธีปฏิบัติในการทดสอบและการนำข้อมูลสำรองจากสื่อบันทึกมาใช้งาน

ข้อ ๕ ต้องทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าข้อมูล รวมทั้งโปรแกรมระบบต่างๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและพร้อมใช้งาน

ข้อ ๖ ต้องจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติต่างๆไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการ-เข้าออก และระบบป้องกันความเสียหายจากสภาพแวดล้อมหรือภัยพิบัติต่างๆ

ข้อ ๗ กำหนดขั้นตอนการทำลายข้อมูลและสื่อบันทึกที่ไม่ได้ใช้งาน

ข้อ ๘ ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม โดยแผนฉุกเฉินมีรายละเอียดดังนี้

๑) ต้องจัดลำดับความสำคัญของระบบงาน และระยะเวลาในการกู้คืนระบบงาน

๒) ต้องกำหนดสถานการณ์หรือลำดับความรุนแรงของปัญหา

๓) ต้องมีขั้นตอนการแก้ไขปัญหาโดยละเอียดในแต่ละสถานการณ์

๔) ต้องกำหนดเจ้าหน้าที่รับผิดชอบ และผู้มีอำนาจในการตัดสินใจ รวมทั้งต้องมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด

๕) ต้องมีรายละเอียดของอุปกรณ์ที่จำเป็นต้องใช้ในกรณีฉุกเฉินของแต่ละระบบงาน เช่น คุณลักษณะของเครื่องคอมพิวเตอร์ (Specification) และอุปกรณ์เครือข่าย เป็นต้น

๖) ในกรณีที่หน่วยงานมีศูนย์คอมพิวเตอร์สำรอง ต้องระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น สถานที่ตั้ง แผนที่ เป็นต้น

๗) ต้องปรับปรุงแผนฉุกเฉินให้เป็นปัจจุบันอยู่เสมอ ควรเก็บแผนฉุกเฉินไว้นอกสถานที่ และต้องทดสอบการปฏิบัติตามแผนฉุกเฉินอย่างน้อยปีละ 1 ครั้ง เป็นการทดสอบในลักษณะการจำลองสถานการณ์จริง เพื่อให้มั่นใจได้ว่าสามารถนำไปใช้ได้จริงในทางปฏิบัติ และต้องมีการบันทึกผลการทดสอบ

๘) แผนฉุกเฉินจะต้องให้บุคคลที่เกี่ยวข้องได้รับทราบเฉพาะเท่าที่จำเป็น

๙) ในกรณีเกิดเหตุการณ์ฉุกเฉิน ควรมีการบันทึกรายละเอียดของเหตุการณ์ สาเหตุของปัญหา และวิธีการแก้ไขปัญหา

ส่วนที่ ๔
แนวปฏิบัติการป้องกันโปรแกรมไม่ประสงค์ดี (Malware)

ข้อ ๑ คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมไม่ประสงค์ดี และต้องปรับปรุงให้ทันสมัยอยู่เสมอ

ข้อ ๒ ผู้ใช้งานควรทำการ update patch หรือ upgrade ซอฟต์แวร์ รวมถึงซอฟต์แวร์ระบบปฏิบัติอย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เพื่อป้องกันการโจมตีจากภัยคุกคาม

ข้อ ๓ ห้ามติดตั้งโปรแกรมหรือซอฟต์แวร์ต่างๆ ที่ได้มาจากแหล่งที่ไม่น่าเชื่อถือ เช่น ได้มาจากเว็บไซต์ที่ให้ดาวน์โหลดซอฟท์แวร์ที่มีการละเมิดลิขสิทธิ์บนอินเทอร์เน็ต หรือติดตั้งโปรแกรมที่เป็นการละเมิดลิขสิทธิ์หรือนโยบายของหน่วยงาน อาจทำให้เครื่องคอมพิวเตอร์มีความเสี่ยงกับโปรแกรมไม่ประสงค์ดี

ข้อ ๔ กรณีที่ต้องแชร์ไฟล์ข้อมูลต่างๆ ให้ทำการแชร์แบบอ่านอย่างเดียว (Read Only) เพื่อป้องกันปัญหาเกี่ยวกับโปรแกรมไม่ประสงค์ดี ถ้าจำเป็นต้องทำการแชร์แบบ Read-Write ให้กำหนดรหัสผ่านสำหรับการแชร์แบบ Write ทุกครั้ง

ข้อ ๕ การใช้สื่อบันทึกพกพา หรือการรับ-ส่งข้อมูลคอมพิวเตอร์ หรือสารสนเทศ (Information) ผ่านทางระบบเครือข่าย ควรมีการตรวจสอบเพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย

ข้อ ๖ ผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย

ข้อ ๗ ผู้ใช้งานควรตรวจสอบไฟล์ที่สามารถประมวลผลได้ (Executable File) เช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe ก่อนทำการเปิดใช้งาน

ส่วนที่ ๕
แนวปฏิบัติการประเมินความเสี่ยง

ข้อ ๑ ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงดังต่อไปนี้

๑) ความเสี่ยงของระบบคอมพิวเตอร์

๒) ความเสี่ยงจากสภาพแวดล้อมทางกายภาพ เช่น ความไม่สงบของบ้านเมือง ระบบไฟฟ้า

๓) ความเสี่ยงที่เกิดจากการปฏิบัติงานของผู้ดูแลระบบและผู้ใช้งาน

๔) ความเสี่ยงของการเข้าถึงสารสนเทศ หรืออุปกรณ์ที่ใช้การประมวลผลสารสนเทศ

๕) ความเสี่ยงต่อการละเมิดทางกฎหมาย

ข้อ ๒ กำหนดวิธีการประเมินความเสี่ยงที่เหมาะสมกับระบบบริหารจัดการของหน่วยงาน กำหนดเกณฑ์ในการยอมรับความเสี่ยง และระบุความเสี่ยงที่ยอมรับได้

ข้อ ๓ การวิเคราะห์และประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๑) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๒) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

๓) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

ข้อ ๔ การประเมินผลในภาพรวมของความเสี่ยงที่ระบุ ต้องจัดทำเป็นคะแนนโดยมีคะแนนเต็ม ๑๐๐ คะแนน และกำหนดให้มีเกณฑ์ในการพิจารณาว่าความเสี่ยงที่ระบุนั้นต้องมีการบริหารจัดการลดความเสี่ยงนั้นหรือไม่ โดยให้เกณฑ์เป็น ๘๐ คะแนนขึ้นไป

ส่วนที่ ๖
แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัย ของระบบเทคโนโลยีสารสนเทศ

ข้อ ๑ จัดให้บุคลากรที่ได้รับมอบหมายดูแลนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ เข้ารับการอบรมอย่างสม่ำเสมอเพื่อให้มีศักยภาพและขีดความสามารถที่จะปฏิบัติงานตามที่กำหนด

ข้อ ๒ จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติตามนโยบายให้กับบุคลากรของสำนักเลขาธิการนายกรัฐมนตรี การจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง และเชิญวิทยากรจากภายนอกที่มีความเชี่ยวชาญ ประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาให้ความรู้กับบุคลากรของหน่วยงาน

ข้อ ๓ เผยแพร่ความรู้เกี่ยวกับแนวปฏิบัติให้กับบุคลากรในสำนักเลขาธิการนายกรัฐมนตรีได้รับทราบในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยผ่านทางระบบเครือข่ายภายในหน่วยงาน (Intranet) และติดประกาศโดยมีการปรับเปลี่ยนเกร็ดความรู้ให้ทันต่อเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

ข้อ ๔ จะต้องมีการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มีการดำเนินการที่เหมาะสมพอเพียงและสัมฤทธิผล

ส่วนที่ ๗
แนวปฏิบัติตามข้อกำหนดทางกฎหมาย

ข้อ ๑ ห้ามมิให้ผู้ใช้งานเผยแพร่รูปภาพที่มีลักษณะลามก อนาจาร ข้อความหมิ่นประมาท ข้อมูลอันเป็นเท็จ หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม ที่ก่อให้เกิดความเสียหายต่อบุคคล สังคม ความมั่นคงทางการเมือง และเศรษฐกิจของประเทศ

ข้อ ๒ ห้ามมิให้ผู้ใช้งานกระทำการใด ๆ โดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น ที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ เช่น การใช้สนิฟเฟอร์ (sniffer)

ข้อ ๓ ห้ามมิให้ผู้ใช้งานส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของ บุคคลอื่น

ข้อ ๔ ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๕ ห้ามใช้ทรัพย์สิน ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของสำนักเลขาธิการนายกรัฐมนตรี เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของสำนักงานเลขาธิการนายกรัฐมนตรี

ข้อ ๖ ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ สำนักเลขาธิการนายกรัฐมนตรีถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๗ หากผู้ใช้งานฝ่าฝืนหรือละเมิดกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้น

เอกสารอ้างอิง

๑. พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

๒. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๓. พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ ๒) พ.ศ. ๒๕๕๑

๔. ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

๕. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕) ประจำปี ๒๕๕๐ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

๖. แผนแม่บท ICT Security แห่งชาติ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ลงวันที่ ๘ กุมภาพันธ์ ๒๕๕๐

๗. คู่มือการรักษาความมั่นคงปลอดภัย ICT กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ๘ กุมภาพันธ์ ๒๕๕๐

๘. ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

๙. แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานภาครัฐ สุรางคณา วายุภาพ ผอ. ฝ่ายกฎหมาย สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

๑๐. แนวทางการจัดเก็บข้อมูลล็อกสำหรับองค์กรเพื่อให้สอดคล้องตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เลอศักดิ์ ลิ้มวิวัฒน์กุล ดร.บรรจง หะรังษี ดร. โกเมน พิบูลย์โรจน์ โปรแกรมเทคโนโลยีเพื่อความมั่นคง วีรยา จุลมณีวงศ์ และ สุรางคณา วายุภาพ ฝ่ายศึกษาวิจัยประเด็นด้านจริยธรรม กฎหมาย และผลกระทบทางสังคมของเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

๑๑. การควบคุมความมั่นคงของข้อมูล และการวัดประสิทธิผลตามข้อกำหนดของมาตรฐาน ISO 27001 http://www.acinfotec.com

๑๒. มาตรฐานการรักษาความมั่นคงปลอดภัย ISO/IEC 27001 และ ISO/IEC 17799 ฉบับประเทศไทย http://www.oknation.net

๑๓. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒) ประจำปี ๒๕๔๙ คณะอนุกรรมการด้านความมั่นคง ในคณะกรรมการธุรกรรมอิเล็กทรอนิส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ