นโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานสภาความมั่นคงแห่งชาติ พ.ศ. 2565

ประกาศสำนักงานสภาความมั่นคงแห่งชาติ

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ประกอบกับตามมาตรา ๔๔ มาตรา ๔๕ ของพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

ดังนั้น เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัย มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์เป็นที่ยอมรับในระดับสากล สำนักงานสภาความมั่นคงแห่งชาติ จึงเห็นควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงานสภาความมั่นคงแห่งชาติ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานสภาความมั่นคงแห่งชาติ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

ข้อ ๒ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย

นโยบายที่ ๑ นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ มีแนวปฏิบัติ ดังนี้

๑) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒) การควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์

๓) การควบคุม...

๓) การเข้าถึงและควบคุมการใช้งานสารสนเทศ
- การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ
- การบริหารจัดการการเข้าถึงของผู้ใช้งาน
- การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
- การควบคุมการเข้าถึงเครือข่าย
- การควบคุมการเข้าถึงระบบปฏิบัติการ
- การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

๔) การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ

๕) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๖) การใช้งานเครื่องคอมพิวเตอร์แบบพกพา

๗) การใช้งานอินเตอร์เน็ต และเครือข่ายสังคมออนไลน์

๘) การใช้งานจดหมายอิเล็กทรอนิกส์

๙) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑๐) การใช้งานระบบไฟร์วอลล์

๑๑) การใช้งานระบบตรวจจับและป้องกันผู้บุกรุก

นโยบายที่ ๒ นโยบายการรักษาสภาพความพร้อมใช้งานของการให้บริการ มีแนวปฏิบัติ ดังนี้

๑) แนวทางปฏิบัติในการสำรองข้อมูล ระบบสำรอง และการปฏิบัติงานในสภาวะฉุกเฉิน

นโยบายที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีแนวปฏิบัติ ดังนี้

๑) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๒) การกำหนดหน้าที่และความรับผิดชอบด้านสารสนเทศ

ข้อ ๓ หน่วยงานต้องจัดทำ **“แผนการรับมือภัยคุกคามทางไซเบอร์”** ให้เป็นไปตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และสอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน

ข้อ ๔ การกำหนดความรับผิดชอบ

๔.๑ เลขาธิการสภาความมั่นคงแห่งชาติ ในฐานะผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) ของสำนักงาน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่สำนักงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๒ ผู้บริหาร...

๔.๒ ผู้บริหารที่ปฏิบัติหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer : DCIO) ของสำนักงาน เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแล และควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๓ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เป็นผู้รับผิดชอบติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ วิธีการ และแนวทางแก้ไขปัญหาแก่เจ้าหน้าที่ระดับปฏิบัติหรือผู้ที่ได้รับมอบหมาย ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๔ เพื่อให้การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานเป็นไปอย่างมีประสิทธิภาพ จึงได้กำหนดให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผู้ดูแลระบบ ผู้รับผิดชอบระบบสารสนเทศ และผู้ที่ได้รับมอบหมาย เป็นผู้รับผิดชอบในการดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวน ปรับปรุงนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานให้เป็นปัจจุบันอยู่เสมอหรืออย่างน้อยปีละ ๑ ครั้ง และหากมีการเปลี่ยนแปลงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานให้ประกาศให้เจ้าหน้าที่ทุกระดับของสำนักงานรับทราบทุกครั้ง

ข้อ ๕ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จัดเป็นมาตรฐานด้านการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์อย่างปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมาย และระเบียบที่เกี่ยวข้อง จึงให้ใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามเอกสารแนบท้ายประกาศนี้ ซึ่งเจ้าหน้าที่ของสำนักงานและผู้เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๑๖ กรกฎาคม พ.ศ. ๒๕๖๕

พลเอก
(สุพจน์ มาลานิยม)
เลขาธิการสภาความมั่นคงแห่งชาติ

เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานสภาความมั่นคงแห่งชาติ พ.ศ. 2565

คำนำ

ระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับสำนักงานในปัจจุบัน เพราะเข้ามาช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ ของสำนักงาน แต่ในขณะเดียวกันก็ทำให้สำนักงานมีความเสี่ยงเพิ่มขึ้นจากภัยคุกคามของระบบเทคโนโลยีสารสนเทศ ซึ่งอาจสร้างความเสียหายต่อการปฏิบัติราชการได้ เนื่องจากระบบเทคโนโลยีสารสนเทศมีการเชื่อมโยงข้อมูลไปยังสำนักงานต่างๆ ส่งผลให้ช่องทางในการถูกบุกรุกเปิดกว้างขึ้นและอาจก่อให้เกิดเหตุอาชญากรรมทางคอมพิวเตอร์กับสำนักงานได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ส่งผลให้สำนักงานสูญเสียชื่อเสียงหรือภาพพจน์ได้ ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

ดังนั้น สำนักงานสภาความมั่นคงแห่งชาติ จึงจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ และเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และให้การดำเนินการของหน่วยงานภายใน เป็นไปในทิศทางเดียวกัน สอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

ทั้งนี้ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานนั้นต้องได้รับความร่วมมือในการปฏิบัติตามอย่างเคร่งครัดและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว จึงหวังเป็นอย่างยิ่งว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของสำนักงานสภาความมั่นคงแห่งชาติทุกคน ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักงานต่อไป

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานสภาความมั่นคงแห่งชาติ

1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานสภาความมั่นคงแห่งชาติ หรือต่อไปนี้เรียกว่า “สำนักงาน” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ สำนักงานจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1 การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ของสำนักงาน ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

1.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO/IEC 27001 พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยของรัฐ (ฉบับที่ 2) พ.ศ. 2556 ที่มีการปรับปรุงอย่างต่อเนื่อง

1.3 นโยบายและแนวปฏิบัตินี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในสำนักงานได้รับทราบและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงาน ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน ในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

1.5 นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย 1 ครั้งต่อปี หรือตามที่ระบุไว้ในเอกสาร “การตรวจสอบประเมินนโยบาย”

2. องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ 1 นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ แนวปฏิบัติที่เกี่ยวข้องมีดังนี้

1) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
2) การควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์
3) การเข้าถึงและควบคุมการใช้งานสารสนเทศ
4) การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
5) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
6) การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
7) การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์
8) การใช้งานจดหมายอิเล็กทรอนิกส์
9) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
10) การใช้งานระบบไฟร์วอลล์
11) การใช้งานระบบตรวจจับและป้องกันผู้บุกรุก

ส่วนที่ 2 นโยบายการรักษาสภาพความพร้อมใช้งานของการให้บริการ แนวปฏิบัติที่เกี่ยวข้องมีดังนี้

1) แนวทางปฏิบัติในการสำรองข้อมูล ระบบสำรอง และการปฏิบัติงานในสภาวะฉุกเฉิน

ส่วนที่ 3 นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ แนวปฏิบัติที่เกี่ยวข้องมีดังนี้

1) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
2) การกำหนดหน้าที่และความรับผิดชอบด้านสารสนเทศ

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ของสำนักงาน เพื่อที่จะทำให้สำนักงานมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน และบุคลากรของสำนักงาน ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน ซึ่งเจ้าหน้าที่ของสำนักงาน หน่วยงานภายนอก และผู้เกี่ยวข้องจะต้องปฏิบัติตามอย่างเคร่งครัด

3. คำนิยาม

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ประกอบด้วยคำนิยาม ดังนี้

สำนักงาน หมายความว่า สำนักงานสภาความมั่นคงแห่งชาติ

หน่วยงานภายใน หมายความว่า สำนักงานเลขาธิการ กอง กลุ่ม กลุ่มงาน สถาบัน ศูนย์ และหน่วยงานอื่นภายในสำนักงาน

ศูนย์ฯ หมายความว่า ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) เป็นหน่วยงานภายในของสำนักงาน ที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ และเครือข่ายภายในสำนักงาน

ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) หมายความว่า เลขาธิการสภาความมั่นคงแห่งชาติ

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer : DCIO) หมายความว่า รองเลขาธิการสภาความมั่นคงแห่งชาติ ที่ปฏิบัติหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม หรือผู้บริหารของสำนักงานที่เลขาธิการสภาความมั่นคงแห่งชาติมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของสำนักงาน

ผู้บังคับบัญชา หมายความว่า ผู้บังคับบัญชาของหน่วยงานภายใน หรือผู้มีอำนาจสั่งการตามโครงสร้างการบริหารราชการของสำนักงาน

ผู้อำนวยการศูนย์ฯ หมายความว่า ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน หรือผู้ที่เลขาธิการสภาความมั่นคงแห่งชาติมอบหมายให้ปฏิบัติหน้าที่ดูแลรับผิดชอบงานของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ผู้ใช้งาน หมายความว่า บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหารจัดการ หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของสำนักงาน โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่กำหนดในการเข้าถึงสารสนเทศของสำนักงาน ดังนี้

- **ผู้บริหาร** หมายความว่า เลขาธิการสภาความมั่นคงแห่งชาติ รองเลขาธิการสภาความมั่นคงแห่งชาติ ผู้ช่วยเลขาธิการสภาความมั่นคงแห่งชาติ ที่ปรึกษาด้านการประสานกิจการความมั่นคง ที่ปรึกษาด้านนโยบายและยุทธศาสตร์ความมั่นคง ผู้อำนวยการกอง/สำนัก/กลุ่ม/สถาบัน/ศูนย์ หัวหน้ากลุ่ม/ศูนย์/กลุ่มงาน
- **ผู้ดูแลระบบ** (System Administrator) หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์
- **ผู้พัฒนาระบบ** หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการพัฒนาระบบแอปพลิเคชัน

- **ผู้ดูแลครุภัณฑ์** หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้เป็นผู้ควบคุมดูแลพัสดุหรือทรัพย์สินของสำนักงานที่อยู่ในความครอบครองของหน่วยงานภายใน ให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลา โดยมิให้เกิดการสูญหาย
- **เจ้าหน้าที่** หมายความว่า ข้าราชการ ลูกจ้างประจำ พนักงานราชการ พนักงานจ้างเหมาบริการ หรือบุคลากรอื่นใดของสำนักงาน
- **บุคคลภายนอก** หมายความว่า บุคคลจากหน่วยงานภายนอกที่เข้ามาประชุมหรือปฏิบัติงานร่วมกับสำนักงาน

หน่วยงานภายนอก หมายความว่า หน่วยงานภายนอกที่สำนักงานอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของสำนักงาน โดยจะได้รับสิทธิในการใช้งานตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เพื่อการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึง การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำสูญหาย ทำให้เสียหาย ถูกทำลายหรือล่วงรู้โดยมิชอบ

มาตรฐาน (Standard) หมายความว่า บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

วิธีการปฏิบัติ (Procedure) หมายความว่า รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ (Guideline) หมายความว่า แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

เจ้าของข้อมูล หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบดูแลข้อมูลโดยตรง โดยเจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่างๆ ที่เกี่ยวข้องกับข้อมูล และได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

สารสนเทศ (Information) หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูล นำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหารจัดการ การวางแผน การตัดสินใจ และอื่นๆ

ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์คอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่เป็นแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ชื่อเครื่องคอมพิวเตอร์ (Computer Name) หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่าย โดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

ระบบเครือข่าย (Network System) หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของสำนักงานได้ เช่น ระบบแลน ระบบอินทราเน็ต ระบบอินเทอร์เน็ต เป็นต้น

- **ระบบแลน** (Local Area Network: LAN) และ**ระบบอินทราเน็ต** (Intranet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในสำนักงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์ เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในสำนักงาน
- **ระบบอินเทอร์เน็ต** (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของสำนักงาน เข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

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

WPA (Wi-Fi Protected Access) หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สาย

VPN (Virtual Private Network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำการเข้ารหัสเฉพาะแล้วรับส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

ไฟร์วอลล์ (Firewall) หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

MAC Address (Media Access Control Address) หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน 16 จำนวน 6 คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

เลขที่อยู่ไอพี (IP Address) หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขที่อยู่ไอพีของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข 4 ส่วน หรือ 6 ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

แผนผังระบบเครือข่าย (Network Diagram) หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของสำนักงาน

อุปกรณ์จัดเส้นทาง (Router) หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ ทำหน้าที่จัดเส้นทางและค้นหาเส้นทาง เพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

ชุดคำสั่งไม่พึงประสงค์ หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือเพิ่มเติม นำมาซึ่งการขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายความว่า ระบบงานของสำนักงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สำนักงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายความว่า พื้นที่ที่สำนักงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

- **พื้นที่ทำงานทั่วไป** (General working area) หมายความว่า พื้นที่ที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน
- **พื้นที่ทำงานของผู้ดูแลระบบ** (System administrator area)
- **พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย** (IT equipment or network area) หมายความว่า พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
- **พื้นที่ควบคุมพิเศษ** หมายความว่า ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server Room) หรือพื้นที่ติดตั้งและจัดวางระบบเครื่องแม่ข่าย อุปกรณ์เชื่อมต่อ และอุปกรณ์เครือข่ายของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ
- **พื้นที่ใช้งานระบบเครือข่ายไร้สาย** (Wireless LAN coverage area)

สินทรัพย์ หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตน ที่มีคุณค่าสำหรับสำนักงาน อันได้แก่ ข้อมูล ระบบข้อมูล ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ ข้อมูลคอมพิวเตอร์และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล อุปกรณ์ต่อพ่วง เป็นต้น

สื่อบันทึกพกพา (Portable Media) หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ CD, DVD, Flash Drive หรือ Thumb Drive หรือ External Hard disk เป็นต้น

จดหมายอิเล็กทรอนิกส์ (e-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อมูลระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3, IMAP และ Exchange เป็นต้น

บัญชีรายชื่อผู้ใช้งาน (User account) หมายความว่า รายชื่อผู้มีสิทธิใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศในระบบเครือข่ายของสำนักงาน

บัญชีชื่อผู้ใช้งาน (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

รหัสผ่าน (Password) หมายความว่า ชุดของตัวอักษรหรืออักขระหรือตัวเลข ที่ถูกกำหนดขึ้นเพื่อใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลที่มีการกำหนดสิทธิการใช้งานไว้ เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

การพิสูจน์ยืนยันตัวตน (Authentication) หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้งานระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งาน ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้บัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password)

ลงบันทึกเข้า (Login) หมายความว่า กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้ถูกต้อง

ลงบันทึกออก (Logout) หมายความว่า กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

การเข้ารหัสลับ (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสลับ เพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมีโปรแกรมถอดรหัสลับ เพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของสำนักงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

ภัยคุกคามทางไซเบอร์ หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ไซเบอร์ หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

ประมวลแนวทางปฏิบัติ หมายความว่า ระเบียบหรือหลักเกณฑ์ที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใดๆ ที่มิชอบ ซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใดๆ เพื่อสร้างความมั่นใจและเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตน ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

หน่วยงานควบคุมหรือกำกับดูแล หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

หมวด 1 การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environment Security)

1. วัตถุประสงค์

กำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ อีกทั้งเพื่อป้องกันทรัพย์สินของสำนักงาน จากการสูญหาย เสียหาย ถูกขโมย หรือโจรกรรม หรือสารสนเทศถูกเปิดเผยโดยมิได้รับอนุญาต โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน

2. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

2.1 สำนักงาน ต้องมีการจำแนกและกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

2.2 ผู้บริหาร ต้องกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT equipment area) พื้นที่ควบคุมพิเศษ และพื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

2.3 ผู้บริหาร ต้องกำหนดสิทธิให้กับเจ้าหน้าที่ ให้สามารถมีสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

2.3.1 จัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

2.3.2 ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่”

2.3.3 จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน

2.3.4 ต้องมีการทบทวนปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่เกี่ยวข้องกับสิทธิการเข้าออกพื้นที่ เช่น การโอน โยกย้าย ลาออก หรือสิ้นสุดการจ้าง

3. การควบคุมการเข้าออก อาคาร สถานที่

3.1 หน่วยงานภายในที่รับผิดชอบด้านความปลอดภัยอาคารและสถานที่ หรือผู้บังคับบัญชาที่รับผิดชอบพื้นที่ หรือผู้ที่ได้รับมอบหมายให้ดูแลสถานที่ ต้องจัดให้มีเจ้าหน้าที่หรือวิธีการรักษาความปลอดภัยเพื่อควบคุมให้เข้าสถานที่ทำงานได้เฉพาะบุคคลที่ได้รับอนุญาตจากเจ้าของพื้นที่เท่านั้น

3.2 จัดทำเอกสารระบุสิทธิของผู้ใช้งานและหน่วยงานภายนอกในการเข้าถึงสถานที่ โดยแบ่งแยกได้ ดังนี้

3.2.1 สำนักงานต้องกำหนดสิทธิผู้ใช้งานที่มีสิทธิผ่านเข้าออก และช่วงเวลาที่มีสิทธิในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร” อย่างชัดเจน

3.2.2 การเข้าถึงอาคารของสำนักงานของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแสดงบัตรที่ใช้ระบุตัวตนที่ส่วนราชการออกให้ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรใน “แบบฟอร์มการเข้าออกพื้นที่” และส่งมอบบัตรผู้ติดต่อ (Visitor)

3.2.3 บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจน ตลอดเวลาที่อยู่ในสำนักงาน

3.2.4 กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำอุปกรณ์ต่างๆ เช่น คอมพิวเตอร์ส่วนบุคคลหรือคอมพิวเตอร์แบบพกพา หรืออุปกรณ์เครือข่ายเข้าบริเวณอาคาร เจ้าหน้าที่รักษาความปลอดภัยจะต้องลงบันทึกในแบบฟอร์มการเข้าออกพื้นที่ในรายการอุปกรณ์ที่นำเข้ามาให้ถูกต้องและชัดเจน

3.2.5 เจ้าหน้าที่ที่บุคคลภายนอกเข้ามาติดต่อ จะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกพื้นที่ให้ถูกต้องและชัดเจน

3.2.6 บุคคลภายนอกหรือผู้ติดต่อ ต้องคืนบัตรผู้ติดต่อ (Visitor) กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบผู้ติดต่อ อุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้องและชัดเจน

3.3 ผู้ใช้งานจะได้รับสิทธิให้เข้าออกสถานที่ทำงานได้ เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้สำหรับปฏิบัติงานเท่านั้น

3.4 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งาน ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานภายในเจ้าของพื้นที่ ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรที่ใช้ระบุตัวตนที่ส่วนราชการออกให้ โดยหน่วยงานภายในเจ้าของพื้นที่ต้องจดบันทึกการขอเข้าออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

4. ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

จัดให้มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของสำนักงานที่เพียงพอต่อความต้องการใช้งาน และมีความพร้อมในการใช้งาน ดังนี้

4.1 ติดตั้งเครื่องกำเนิดกระแสไฟฟ้าสำรอง

4.2 ติดตั้งระบบระงับเพลิง

4.3 ติดตั้งระบบปรับอากาศและควบคุมความชื้น

4.4 ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องแม่ข่ายทำงานผิดปกติ หรือหยุดการทำงาน

4.5 วางแผนการตรวจสอบ บำรุงรักษา ระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของสำนักงานอย่างสม่ำเสมอ ให้มั่นใจได้ว่าระบบต่างๆ สามารถทำงานได้ตามปกติ

5. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

5.1 หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของสำนักงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้ กรณีต้องผ่านพื้นที่ที่มีความเสี่ยงต้องติดตั้งระบบป้องกันที่ปลอดภัย

5.2 ให้มีการร้อยท่อสายสัญญาณต่างๆ หรือมีการป้องกันโดยวิธีอื่นที่เหมาะสม เพื่อป้องกันการตัดสายสัญญาณทำให้เกิดความเสียหาย หรือการดักรับข้อมูลโดยผู้ที่มิได้รับอนุญาต

5.3 สายไฟต้องแยกจากสายสื่อสารในระยะที่เหมาะสม เพื่อป้องกันการรบกวนของสัญญาณ

5.4 ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่างๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

5.5 จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

5.6 ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

5.7 พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม เช่น สายสัญญาณแบบ Coaxial Cable สำหรับระบบสารสนเทศที่สำคัญ

5.8 ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี 3 เดือน / 6 เดือน สำหรับสายไฟเบอร์ออฟติก

6. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

6.1 วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา และต้องมีการซ่อมบำรุงอย่างทันท่วงทีตามความสำคัญของระบบ

6.2 บันทึกประวัติการบำรุงรักษาและซ่อมบำรุงอุปกรณ์ทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง โดยมีรายละเอียด ดังนี้ วันที่บำรุงรักษาและซ่อมบำรุง รายการอุปกรณ์ สถานะของอุปกรณ์ ปัญหาที่พบและการแก้ไข ผู้ดำเนินการบำรุงรักษาและซ่อมบำรุงพร้อมลงลายมือชื่อ

6.3 ถ้ามีการจัดจ้างหน่วยงานหรือผู้ให้บริการภายนอก เพื่อบำรุงรักษาและซ่อมบำรุงอุปกรณ์ หน่วยงานภายในที่จัดจ้างต้องจัดให้มีสัญญาหรือข้อตกลงการจ้าง โดยต้องกำหนดระยะเวลา ขอบเขต และระดับการให้บริการอย่างชัดเจน

6.4 ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในสำนักงาน ในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษ ผู้ดูแลระบบหรือผู้รับผิดชอบการซ่อมบำรุงอุปกรณ์จะต้องอยู่ในพื้นที่ทุกครั้ง

6.5 จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างหรือผู้ให้บริการภายนอกที่เข้ามาบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

7. การนำทรัพย์สินของสำนักงานออกนอกสำนักงาน (Removal of Property)

7.1 หน่วยงานภายในต้องมอบหมายเจ้าหน้าที่เป็น “ผู้ดูแลครุภัณฑ์” มีหน้าที่ควบคุมดูแลพัสดุหรือทรัพย์สินของสำนักงานที่อยู่ในความครอบครอง ให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลา โดยมิให้เกิดการสูญหาย และจัดทำ “ทะเบียนครุภัณฑ์” ของหน่วยงานภายใน บันทึกว่าถูกใช้ประจำอยู่ที่ใคร และสถานภาพและการเคลื่อนย้ายของครุภัณฑ์ ทั้งนี้ ต้องตรวจสอบสถานภาพของครุภัณฑ์อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง การเคลื่อนย้าย เช่น ได้รับมอบครุภัณฑ์เพิ่มเติม การตัดจำหน่าย การเปลี่ยนผู้ครอบครอง การยืม การโอน หรือการส่งซ่อม

7.2 ต้องขออนุญาตจากผู้บังคับบัญชาของหน่วยงานภายในและแจ้งให้ผู้ดูแลครุภัณฑ์ทราบก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานภายนอกสำนักงาน หรือนำไปซ่อมบำรุงที่ศูนย์ฯ

7.3 ต้องได้รับความเห็นชอบจากผู้อำนวยการศูนย์ฯ ก่อนนำครุภัณฑ์คอมพิวเตอร์ส่งซ่อมภายนอกสำนักงาน

7.4 การให้ยืมอุปกรณ์หรือทรัพย์สิน ผู้ดูแลครุภัณฑ์จะต้องตรวจสอบ ติดตามให้ทรัพย์สินดังกล่าวนำกลับมาตามช่วงเวลาที่กำหนด และอยู่ในสภาพดี หรือไม่ต่างจากตอนที่ถูกยืม และต้องบันทึกข้อมูลการนำอุปกรณ์ของสำนักงานออกไปใช้งานนอกสำนักงาน และบันทึกส่งคืน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย

8. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of Equipment off Premises)

8.1 กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของสำนักงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

8.2 ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของสำนักงานไว้โดยลำพังในที่สาธารณะ เสี่ยงต่อการสูญหาย

8.3 เจ้าหน้าที่ผู้ใช้งานต้องรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

9. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

9.1 การจำหน่ายครุภัณฑ์คอมพิวเตอร์ อุปกรณ์เครือข่าย หน่วยงานภายในที่เป็นเจ้าของทรัพย์สิน ต้องจัดให้มีการทำลายข้อมูลและซอฟต์แวร์ลิขสิทธิ์ในสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ก่อนการจำหน่าย เพื่อให้มั่นใจว่าข้อมูลและซอฟต์แวร์ลิขสิทธิ์จะไม่สามารถนำกลับมาใช้ได้อีก (Non - Retrievable)

9.2 ผู้อำนวยการศูนย์ฯ เป็นผู้อนุมัติในการกำจัดหรือนำอุปกรณ์สารสนเทศกลับมาใช้ โดยผู้ที่ต้องการกำจัด หรือนำอุปกรณ์สารสนเทศกลับมาใช้ ต้องยื่นเรื่องเป็นลายลักษณ์อักษรเพื่อขออนุมัติ

9.3 ต้องทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว โดยต้องมั่นใจว่าข้อมูลดังกล่าวจะไม่สามารถนำกลับมาใช้ได้อีก

หมวด 2 การควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์
(Computer Center Entry Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกัน มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของสำนักงาน โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่างๆ ที่มีความจำเป็นต้องเข้าออกห้องศูนย์คอมพิวเตอร์

2. คำจำกัดความของผู้เกี่ยวข้อง

2.1 ผู้ดูแลระบบ หมายความว่า เจ้าหน้าที่ที่ปฏิบัติงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในศูนย์ฯ

2.2 เจ้าหน้าที่ศูนย์ฯ หมายความว่า เจ้าหน้าที่ของสำนักงานที่ปฏิบัติงานภายในศูนย์ฯ

2.3 เจ้าหน้าที่ หมายความว่า เจ้าหน้าที่ของสำนักงานที่มีสิทธิในการเข้าออกสถานที่/อาคาร/ห้องภายในสำนักงาน

2.4 ผู้ติดต่อหรือบุคคลภายนอก หมายความว่า บุคคลจากหน่วยงานภายนอกที่มาติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่างๆ ของศูนย์ฯ หรือผู้รับจ้างที่เข้ามาซ่อมบำรุงอุปกรณ์ภายในศูนย์ฯ

3. บทบาทและความรับผิดชอบ

3.1 ผู้อำนวยการศูนย์ฯ

3.1.1 อนุมัติสิทธิการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

3.1.2 อนุมัติกระบวนการควบคุมการเข้าออกศูนย์ฯ

3.2 ผู้ดูแลระบบ

3.2.1 ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในศูนย์ฯ ให้ปฏิบัติตามระเบียบและกฎเกณฑ์อย่างเคร่งครัด

3.2.2 ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกศูนย์ฯ ต้องติดบัตรผู้ติดต่อ (Visitor) หรือบัตรประจำตัวของสำนักงานเท่านั้น

4. กระบวนการควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์

4.1 ผู้ดูแลระบบ เจ้าหน้าที่ศูนย์ฯ และเจ้าหน้าที่ของสำนักงาน มีแนวทางปฏิบัติ ดังนี้

4.1.1 ผู้ดูแลระบบ ต้องจัดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นสัดส่วนชัดเจน เช่น พื้นที่ควบคุมส่วนระบบเครือข่าย (Network Zone) พื้นที่ควบคุมพิเศษส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น เพื่อสะดวกในกาปฏิบัติงานและยังทำให้การควบคุมการเข้าถึง หรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่างๆ มีประสิทธิภาพมากขึ้น

4.1.2 ผู้อำนวยการศูนย์ฯ ต้องอนุมัติสิทธิในการเข้าออกพื้นที่ศูนย์ฯ และการเข้าถึงพื้นที่ควบคุมพิเศษ เจ้าหน้าที่ที่ปฏิบัติหน้าที่ภายในศูนย์ฯ และมีการบันทึก "ทะเบียนผู้มีสิทธิเข้าออกพื้นที่" เช่น ผู้ดูแลระบบ (System Administrator) เจ้าหน้าที่ศูนย์ฯ เป็นต้น

4.1.3 สิทธิในการเข้าออกห้องต่างๆ ภายในศูนย์ฯ ของเจ้าหน้าที่ศูนย์ฯ แต่ละคน ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์ฯ โดยผ่านกระบวนการลงทะเบียนที่ระบุไว้ในเอกสาร "การบริหารจัดการสิทธิการใช้งานระบบ" เป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับภารกิจและหน้าที่รับผิดชอบในการปฏิบัติงานภายในศูนย์ฯ

4.1.4 เจ้าหน้าที่ศูนย์ฯ ทุกคนต้องทำบัตรผ่านเพื่อใช้ในการเข้าออกศูนย์ฯ ตามกระบวนการที่ระบุในเอกสาร "การบริหารจัดการสิทธิการใช้งานระบบ" หรือยืนยันตัวตนด้วยระบบการสแกนลายนิ้วมือ

4.1.5 ต้องจัดทำระบบเก็บบันทึกการเข้าออกพื้นที่ศูนย์ฯ ตามกระบวนการที่ระบุไว้ในเอกสาร "บันทึกการเข้าออกพื้นที่"

4.1.6 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออกศูนย์ฯ ต้องมีการควบคุมอย่างรัดกุม

4.1.7 การเข้าถึงพื้นที่ศูนย์ฯ และพื้นที่ควบคุมพิเศษ ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร "บันทึกการเข้าออกพื้นที่"

4.1.8 เจ้าหน้าที่ศูนย์ฯ ทุกคนต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้าออกทุกคนต้องกรอกแบบฟอร์มดังกล่าว

4.2 ผู้ติดต่อหรือบุคคลภายนอก มีแนวทางปฏิบัติดังนี้

4.2.1 ผู้ติดต่อหรือบุคคลภายนอกทุกคนต้องทำการแสดงบัตรที่ใช้ระบุตัวตนที่ส่วนราชการออกให้ กับเจ้าหน้าที่รักษาความปลอดภัย และทำการลงบันทึกข้อมูลบัตรใน “แบบฟอร์มการเข้าออกพื้นที่” เพื่อรับบัตรผู้ติดต่อ (Visitor)

4.2.2 ผู้ติดต่อหรือบุคคลภายนอกที่จะเข้าปฏิบัติงาน หรือนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในสำนักงาน จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร "บันทึกการเข้าออกพื้นที่" ให้ถูกต้องชัดเจนโดยเจ้าหน้าที่รักษาความปลอดภัย

4.2.3 ผู้ติดต่อหรือบุคคลภายนอก ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในศูนย์ฯ

4.2.4 ผู้ติดต่อหรือบุคคลภายนอก จะสามารถเข้าออกศูนย์ฯ ได้ ต้องมีเจ้าหน้าที่ศูนย์ฯ เป็นผู้เปิดประตูให้

4.2.5 พื้นที่ที่ผู้ติดต่อหรือบุคคลภายนอก สามารถเข้าถึงได้ตามที่ระบุไว้ในแบบฟอร์มการเข้าออกพื้นที่ และต้องมีเจ้าหน้าที่ศูนย์ฯ คอยสอดส่องดูแลตลอดเวลา

4.2.6 ผู้ติดต่อหรือบุคคลภายนอก สามารถนำผู้ติดตามเข้ามาช่วยงานได้ไม่เกินครั้งละ 2 คน และทุกคนจะต้องถูกบันทึกการเข้าออกเช่นกัน

4.2.7 ผู้ติดต่อหรือบุคคลภายนอก ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัย ซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตรทุกครั้ง

4.2.8 เจ้าหน้าที่รักษาความปลอดภัย ต้องตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในแบบฟอร์มการเข้าออกพื้นที่ และตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง

4.2.9 เจ้าหน้าที่ศูนย์ฯ ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการเข้าออกพื้นที่กับเจ้าหน้าที่รักษาความปลอดภัย เป็นประจำทุกเดือน

4.2.10 เจ้าหน้าที่ศูนย์ฯ ต้องทำการทบทวนสิทธิของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การย้าย โอน ลาออก หรือสิ้นสุดสัญญาจ้าง

หมวด 3 การเข้าถึงและควบคุมการใช้งานสารสนเทศ
(access control)

1. วัตถุประสงค์

1.1 เพื่อให้ข้อมูลที่มีความสำคัญต่อสำนักงาน ได้รับการจำแนกชั้นความลับอย่างเหมาะสมตามระดับความสำคัญของข้อมูล และเพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องรับรู้และสามารถนำข้อมูลแต่ละชั้นความลับไปใช้งานได้อย่างถูกต้องและเหมาะสม

1.2 เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาต เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานได้อย่างถูกต้อง

2. การกำหนดลำดับความสำคัญของข้อมูลและการใช้งานข้อมูล

2.1 สำนักงานใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ โดยมีการแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ดังนี้

2.1.1 จัดแบ่งประเภทของข้อมูล ออกเป็น

1) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

2) ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลการขอใช้รถยนต์ส่วนกลาง ข้อมูลการขอใช้ห้องประชุม เอกสารเผยแพร่บนเว็บไซต์ของสำนักงาน

2.1.2 การรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้ การเข้าถึงข้อมูลแต่ละประเภทต้องเป็นไปตามระดับชั้นความลับของสำนักงาน ดังต่อไปนี้

1) ลับมาก (Secret) มีความสำคัญต่อสำนักงานในระดับสูงมาก หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อสำนักงานอย่างมาก

2) ลับที่สุด (Confidential) มีความสำคัญต่อสำนักงานในระดับสูง หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อสำนักงานอย่างมีนัยยะสำคัญ

3) ใช้ภายในสำนักงาน (Internal Use) เป็นข้อมูลที่อนุญาตให้ใช้ภายในสำนักงาน หากข้อมูลสูญหายหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต จะส่งผลเสียหายต่อสำนักงาน

4) สาธารณะ (Public) เป็นข้อมูลที่ใช้เผยแพร่สู่สาธารณะ การเปิดเผยข้อมูลประเภทนี้ไม่ส่งผลกระทบใดกับสำนักงาน

2.1.3 การจัดแบ่งระดับชั้นการเข้าถึง

ระดับที่ 1 ระดับชั้นสำหรับผู้บริหาร

ระดับที่ 2 ระดับชั้นสำหรับผู้ใช้งานทั่วไป

ระดับที่ 3 ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

2.1.4 กำหนดเวลาที่สามารถเข้าถึงได้ตลอดเวลา 24 ชั่วโมง 7 วัน รวมทั้ง การเข้าถึงระบบอย่างมีเงื่อนไข **(รายละเอียดตามผนวก)**

2.1.5 การกำหนดช่องทางในการเข้าถึงข้อมูล ผู้ใช้งานที่สามารถเข้าถึงข้อมูลตามช่องทางการเข้าถึงที่กำหนดไว้นั้น จะต้องได้รับสิทธิจากสำนักงาน โดยมีการกำหนดบัญชีชื่อผู้ใช้งานตามระดับชั้นการเข้าถึง ให้สามารถเข้าใช้งานตามประเภทความรับผิดชอบ สิทธิในการเข้าถึงข้อมูลและสามารถเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตเท่านั้น

2.2 การใช้งานข้อมูล

2.2.1 ผู้ใช้งานทุกคนต้องใช้งานข้อมูลของสำนักงานตามกฎระเบียบและคำแนะนำที่สำนักงานกำหนดไว้

2.2.2 ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษในการใช้งานข้อมูลประเภทลับมาก และลับที่สุด (ต่อไปในเอกสารนี้เรียกว่า “ข้อมูลลับ”) เพื่อป้องกันไม่ให้ข้อมูลถูกเข้าถึงหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต

2.2.3 ข้อมูลลับของสำนักงานต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น (ตามหลักการ “Need to Know”)

2.2.4 ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลลับที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง เครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการหรือแอปพลิเคชันอย่างเหมาะสม

2.2.5 ข้อมูลใดที่ผู้ใช้งานพิจารณาว่าเป็นข้อมูลลับหรือมีจุดอ่อนด้านความมั่นคงปลอดภัยต้องได้รับการเข้ารหัส

2.2.6 ผู้ใช้งานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับ ในตู้ที่สามารถปิดล็อคได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่ง เมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อนั้นไว้ โดยไม่อยู่ที่โต๊ะทำงาน

2.2.7 ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่างๆ เช่น เครื่องพิมพ์ เครื่องโทรสาร เครื่องถ่ายเอกสาร ฯลฯ ทันที

2.2.8 ผู้ใช้งานต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

2.2.9 ผู้ใช้งานต้องไม่พูดคุยหรือใช้งานข้อมูลลับของสำนักงานในพื้นที่สาธารณะ เช่น ลิฟต์ ร้านอาหาร ฯลฯ

3. กระบวนการหลักในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

3.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็น ผ่านเข้าใช้งานได้เท่านั้น

3.2 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงาน ก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชาและผู้ดูแลระบบตามความจำเป็นในการใช้งาน

3.2.1 กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

1) อ่านอย่างเดียว
2) สร้างข้อมูล หรือนำเข้าข้อมูล
3) แก้ไขข้อมูล
4) ลบข้อมูล
5) อนุมัติ
6) ไม่มีสิทธิ

3.3 ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

3.4 ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

3.5 ผู้ดูแลระบบต้องจัดให้มีการบันทึกประวัติการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

4. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

4.1 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบแก่ผู้ใช้งานในการขออนุญาตเข้าใช้ระบบงานนั้น จะต้องมีบันทึกเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและมีการลงนามอนุมัติโดยผู้บังคับบัญชา เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

4.2 ผู้ดูแลระบบต้องกำหนดระยะเวลาการเชื่อมต่อเข้าสู่ระบบสารสนเทศ/แอปพลิเคชันที่มีความสำคัญ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

4.3 เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่รับผิดชอบเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

4.4 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

5. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

5.1 สร้างความรู้ ความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้ใช้งาน

5.1.1 สำนักงาน จัดให้มีการอบรมเพื่อสร้างความรู้และความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ และรู้เท่าทันต่อภัยคุกคามและผลกระทบที่อาจจะเกิดขึ้น จากการใช้งานระบบสารสนเทศอย่างไม่ระมัดระวัง โดยจัดให้มีการอบรมผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง

5.1.2 กรณีเป็นผู้ใช้งานจากภายนอกที่ได้รับสิทธิเพื่อเข้าใช้งานระบบสารสนเทศ จะต้องได้รับการชี้แจงและทำความเข้าใจเรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เมื่อได้รับสิทธิการเข้าใช้งานระบบสารสนเทศของสำนักงาน

5.2 การลงทะเบียนเจ้าหน้าที่ใหม่ของสำนักงาน ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่ เพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกหรือเปลี่ยนแปลงสิทธิการใช้งาน

5.3 การลงทะเบียนผู้ใช้งาน (user registration)

5.3.1 ผู้ดูแลระบบจัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศ

5.3.2 ผู้ดูแลระบบต้องตรวจสอบบัญชีรายชื่อผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

5.3.3 ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบตามรายละเอียดสิทธิในแต่ละภารกิจ

5.3.4 ผู้ดูแลระบบต้องชี้แจงและแจ้งผู้ใช้งานเป็นลายลักษณ์อักษร เพื่อให้ผู้ใช้งานทราบถึงสิทธิหน้าที่รับผิดชอบ และมาตรการรด้านความมั่นคงปลอดภัยในการเข้าถึงระบบสารสนเทศ

5.3.5 กำหนดให้มีการยกเลิก เพิกถอนการอนุญาตเข้าถึงระบบสารสนเทศ การตัดออกจากทะเบียนผู้ใช้งาน เมื่อได้รับแจ้งจากต้นสังกัดหรือเมื่อมีการเปลี่ยนแปลงตำแหน่ง โยกย้าย ลาออก หรือสิ้นสุดการจ้าง เป็นต้น

5.4 การบริหารจัดการสิทธิผู้ใช้งาน (User Management)

5.4.1 กำหนดระดับสิทธิการเข้าถึงระบบสารสนเทศตามหน้าที่รับผิดชอบและความจำเป็นในการใช้งาน และทบทวนสิทธิอย่างสม่ำเสมอหรืออย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่ง โยกย้าย ลาออก หรือสิ้นสุดการจ้าง เป็นต้น

5.4.2 ผู้ดูแลระบบต้องปรับปรุงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศตามหน้าที่รับผิดชอบและจัดเก็บข้อมูลการกำหนดสิทธิให้แก่ผู้ใช้งานไว้เป็นฐานข้อมูล

5.4.3 ในกรณีที่ต้องให้สิทธิพิเศษนอกเหนือจากภาระงานที่กำหนด จะต้องได้รับการอนุมัติเห็นชอบจากต้นสังกัด และผู้อำนวยการศูนย์ฯ จัดทำคำร้องเป็นลายลักษณ์อักษร โดยการให้สิทธิพิเศษดังกล่าวจะต้องกำหนดช่วงเวลาที่ชัดเจน และเมื่อพ้นกำหนดการให้สิทธิพิเศษแล้วจะต้องระงับการใช้งานทันที

5.5 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

5.5.1 ผู้ดูแลระบบกำหนดรหัสผ่านชั่วคราวในครั้งแรกให้แก่ผู้ใช้งาน ส่งมอบให้ผู้ใช้งานเป็นเอกสารปิดผนึกที่เป็นความลับหรือทางจดหมายอิเล็กทรอนิกส์ (e-mail) เมื่อผู้ใช้งานได้รับจะต้องเปลี่ยนรหัสผ่านใหม่ทันที ภายใน 7 วัน

5.5.2 การตั้งรหัสผ่านใหม่จะต้องตั้งรหัสให้มีความยากในการคาดเดา โดยรหัสผ่านต้องมีความยาวอย่างน้อย 8 ตัวอักขระ (digits) ประกอบด้วยตัวอักษรตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์

5.5.3 กำหนดให้การเข้ารหัสผิดพลาดได้ไม่เกิน 3 ครั้ง ระบบจะต้องล็อคสิทธิการเข้าถึงของผู้ใช้งาน โดยผู้ใช้งานจะต้องแจ้งความจำนงให้ผู้ดูแลระบบปลดล็อคหรือรีเซ็ตรหัสผ่านใหม่

5.5.4 กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ทุกๆ 180 วัน

5.6 กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาและผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

5.7 ผู้ใช้งานต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

5.8 การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่านของเจ้าหน้าที่

5.8.1 ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

5.8.2 การกำหนด การเปลี่ยนแปลง และการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

5.8.3 กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ซึ่งผู้ใช้งานที่มีสิทธิสูงสุด จะต้องพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

1) ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้นๆ
2) ต้องควบคุมการใช้งานอย่างเข้มงวด กำหนดการใช้งานเฉพาะกรณีจำเป็นเท่านั้น
3) ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
4) ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานควรเปลี่ยนรหัสผ่านทุก 3 เดือน เป็นต้น

5.9 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

5.9.1 ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

5.9.2 เจ้าของข้อมูลจะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ อย่างน้อยปีละ 4 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

5.9.3 วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบ ต้องกำหนดบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

5.9.4 การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

5.9.5 ต้องกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

5.9.6 ต้องมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของสำนักงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลก่อน เป็นต้น

5.10 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

5.10.1 การใช้งานรหัสผ่าน (Password Use)

1) ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน

2) การกำหนดรหัสผ่าน (Password) ที่เดาสุ่มได้ยาก ซึ่งประกอบด้วย

- กำหนดให้มีความยาวไม่น้อยกว่า 8 ตัวอักษร
- ใช้อักขระพิเศษประกอบ เช่น :;<> เป็นต้น
- ไม่กำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef”, “aaaaa” เป็นต้น
- การกำหนดรหัสผ่านใหม่ต้องไม่ซ้ำกับของเดิมครั้งสุดท้าย
- ไม่กำหนดรหัสผ่านที่เกี่ยวข้องผู้ใช้งาน เช่น ชื่อ นามสกุล หรือวันเกิด เป็นต้น
- ไม่กำหนดรหัสผ่านที่เป็นคำศัพท์ในพจนานุกรม
- ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือบุคคลในครอบครัว

3) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
4) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
5) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน 180 วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

5.10.2 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ มีการกำหนดมาตรการป้องกันทรัพย์สินของสำนักงาน และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญ ให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่างๆ คือ การจัดการบริเวณล้อมรอบ การควบคุมการเข้าออก การจัดวางอุปกรณ์ระบบและอุปกรณ์สนับสนุนการทำงานในสถานที่ที่มีความปลอดภัย ดังนี้

1) ผู้ดูแลระบบหรือผู้รับผิดชอบ ต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศ และการเข้าใช้งานคอมพิวเตอร์ทันทีเมื่อเสร็จสิ้นการใช้งานหรือพักการใช้งานชั่วคราว เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
2) ผู้ใช้งานจะต้องป้องกันและดูแลอุปกรณ์คอมพิวเตอร์และเครือข่ายของสำนักงานตลอดเวลา เพื่อไม่ให้เกิดความเสียหาย สูญหาย หรือมีผู้ไม่ประสงค์ดีเข้าถึงระบบและอุปกรณ์ต่างๆ โดยไม่ได้รับอนุญาต
3) กำหนดค่าให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 10 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้
4) กำหนดรหัสผ่านสำหรับการเข้าใช้งานเครื่องคอมพิวเตอร์ และต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งไว้ โดยไม่ได้ดูแลชั่วคราว
5) การใช้งานเครื่องแม่ข่ายหรือระบบคอมพิวเตอร์ เมื่อเสร็จสิ้นแล้วจะต้องทำการ log off ทุกครั้ง
6) มีการควบคุมการเข้าออกพื้นที่ โดยผู้ไม่มีส่วนเกี่ยวข้องต้องได้รับอนุญาตก่อนการเข้าถึงพื้นที่ปฏิบัติงาน

5.10.3 การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) สำนักงานได้กำหนดแนวปฏิบัติเพื่อควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ โดยมีแนวปฏิบัติ ดังนี้

1) ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน หรือเมื่อมีเหตุให้ว่างเว้นจากการใช้งาน

2) ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอขณะที่ไม่ได้ใช้งานภายในระยะเวลา 10 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิด หน้าจอได้
3) ผู้ใช้งานต้องล็อกใส่รหัสผ่านป้องกันการเข้าถึงอุปกรณ์ สื่อบันทึกข้อมูล และเครื่องคอมพิวเตอร์ที่สำคัญเมื่อไม่ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว
4) กรณีข้อมูลสำคัญที่บันทึกไว้ใน กระดาษ สื่อบันทึกข้อมูลแฟลชไดร์ฟหรือฮาร์ดดิสก์เมื่อไม่ใช้งาน ต้องจัดเก็บไว้ในที่ปลอดภัย ไม่วางทิ้งไว้บนโต๊ะทำงานโดยไม่มีผู้ดูแล
5) ผู้ใช้งานต้องทำความเข้าใจในการป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์และสร้างความตระหนักในการที่จะต้องปฏิบัติตามแนวปฏิบัติอย่างเคร่งครัด
6) การทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลาย ดังนี้

ลำดับ	ประเภทสื่อบันทึกข้อมูล	แนวทางการทำลาย
1	- แฟลชไดรฟ์ (Flash Drive) - ฮาร์ดดิสก์ (Hard disk) - ฮาร์ดดิสก์พกพา (External Hard disk)	- ทำลายข้อมูลตามแนวทางของ DOD 5220.22-M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายๆ รอบ - ทุบทำลาย หรือบดให้อุปกรณ์เสียหายไม่สามารถนำไปใช้งานได้
2	แผ่นซีดี / ดีวีดี (CD/DVD)	ใช้วิธีการตัด เผา ทำให้สิ้นสภาพการใช้งาน
3	เทป	ใช้วิธีทุบ ทำลายให้เสียหายสิ้นสภาพการใช้งาน
4	กระดาษ	ตัดด้วยเครื่องทำลายเอกสาร

7) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 โดยการรับ-ส่งข้อมูลสำคัญ หรือข้อมูลซึ่งเป็นความลับให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล SSL หรือ VPN
8) มีการจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก และต้องมีผู้รับผิดชอบคอยควบคุมดูแลตลอดระยะเวลาการส่งมอบ ไม่ปล่อยให้บุคคลภายนอกอยู่ตามลำพังในพื้นที่ปฏิบัติงาน

5.10.4 การใช้งานระบบสารสนเทศอย่างปลอดภัย เพื่อให้การใช้งานระบบสารสนเทศมีความปลอดภัย และไม่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศของสำนักงาน กำหนดแนวทางปฏิบัติสำหรับผู้ใช้งาน ดังนี้

1) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้ง ก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของสำนักงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล็อคหรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที
2) ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของสำนักงาน หรือเป็นบุคคลภายนอก

3) การกระทำใดๆ ที่เกิดจากการใช้บัญชีชื่อผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง
4) ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของสำนักงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บริหารระดับสูงสุดของสำนักงาน
5) ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคล โดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่สำนักงานต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับสำนักงาน ซึ่งสำนักงานอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ
6) ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หมายถึง วิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หรือหมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิตทอร์เรนต์ (BitTorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บริหารระดับสูงสุดของสำนักงาน
7) ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น
8) ห้ามใช้สินทรัพย์ของสำนักงานที่จัดเตรียมให้ เพื่อการเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของสำนักงาน
9) ห้ามใช้ระบบสารสนเทศของสำนักงาน เพื่อรบกวนก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของสำนักงาน
10) ห้ามใช้ระบบสารสนเทศของสำนักงานเพื่อประโยชน์ทางการค้า
11) ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายของสำนักงานโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

5.11 การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirement for access control)

เพื่อเป็นการควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศของสำนักงาน และการปรับปรุงเพื่อให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัยการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศมีแนวปฏิบัติ ดังนี้

5.11.1 การควบคุมการเข้าถึงสารสนเทศ

1) ผู้ดูแลระบบ รับผิดชอบให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของสำนักงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

2) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบภายหลัง

5.11.2 ข้อกำหนดการใช้งานตามภารกิจ

เพื่อให้การเข้าถึงและใช้งานสารสนเทศสอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย จึงจำแนกกลุ่มผู้ใช้งานและกำหนดให้มีการแบ่งกลุ่มตามสิทธิ และภารกิจ ดังนี้

- กลุ่มผู้บริหาร กำหนดสิทธิการเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายในการกำกับดูแล เช่น สิทธิการอนุมัติ สิทธิการเข้าถึงรายงานสรุปผล
- กลุ่มของผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร กำหนดสิทธิการเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายจากผู้อำนวยการศูนย์ฯ เช่น สิทธิในการกำหนดสิทธิการเข้าใช้งานของผู้ใช้งานในแต่ละระบบตามที่ผู้บังคับบัญชามอบหมาย
- กลุ่มผู้ใช้งาน กำหนดสิทธิการเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายจากผู้บังคับบัญชาของหน่วยงานภายใน เช่น สิทธิการเพิ่ม/แก้ไข/ลบข้อมูล ที่อยู่ในความรับผิดชอบ
- กลุ่มเจ้าหน้าที่ของสำนักงาน กำหนดสิทธิให้สามารถเข้าถึงข้อมูลทั่วไป เช่น สิทธิการอ่านอย่างเดียว
- กลุ่มที่ปรึกษาจากภายนอกหรือผู้รับจ้างที่มีระยะสัญญาจ้างกับสำนักงาน กำหนดสิทธิเฉพาะกิจตามความจำเป็นที่ต้องเข้าถึงข้อมูล
- ผู้ใช้งานที่เข้ามาใช้ระบบสารสนเทศชั่วคราว (Guest) ไม่มีสิทธิในการเข้าถึง

6. การควบคุมการเข้าถึงเครือข่าย (network access control)

6.1 ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

6.2 การเข้าสู่ระบบเครือข่ายภายในของสำนักงาน โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์ฯ ก่อนที่จะสามารถใช้งานได้ในทุกกรณี

6.3 การเข้าถึงระบบเครือข่ายหรือระบบเทคโนโลยีสารสนเทศภายในของสำนักงาน ต้องดำเนินการโดยใช้อุปกรณ์ที่สำนักงานเป็นผู้จัดหา หรืออุปกรณ์ที่ได้รับอนุญาตซึ่งผ่านการลงทะเบียน

6.4 อุปกรณ์ที่ใช้ในการเข้าถึงระบบเครือข่ายภายในของสำนักงาน ต้องได้รับการพิสูจน์ตัวตนด้วยวิธีการที่เหมาะสม ได้แก่ การตรวจสอบความถูกต้องของ Media Access Control Address (MAC) การตรวจสอบความถูกต้องของรหัสประจำเครื่อง หรือการตรวจสอบ Digital Certificate ของอุปกรณ์ เป็นต้น

6.5 ผู้ดูแลระบบต้องควบคุมพอร์ตของอุปกรณ์ต่างๆ ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ โดยมีรายละเอียดดังนี้

6.5.1 พอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Diagnostic และ Configuration Port) ต้องถูกจำกัดให้สามารถใช้งานได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น

6.5.2 การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ต้องดำเนินการผ่านโพรโทคอลที่มีความมั่นคงปลอดภัย เช่น Secure Shell (SSH) หรือผ่านระบบเครือข่ายแบบ Out-of-band เท่านั้น

6.5.3 การเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบจากระยะไกลผ่านเครือข่ายภายนอก ต้องได้รับการพิสูจน์ตัวตนของผู้ใช้งาน ด้วยวิธีการตรวจสอบตั้งแต่ 2 ประเภทขึ้นไป (two factors authentication) และใช้ช่องทางการเชื่อมต่อที่มั่นคงปลอดภัย

6.5.4 พอร์ตที่ไม่เกี่ยวข้องกับการปฏิบัติงานหรือการดำเนินภารกิจต้องถูกระงับการใช้งาน

6.6 ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งาน ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

6.7 ผู้ดูแลระบบ ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

6.8 ผู้ดูแลระบบ ต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้

6.9 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละ 1 ครั้ง นอกจากนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

6.10 ระบบเครือข่ายทั้งหมดของสำนักงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกสำนักงาน ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

6.11 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสำนักงานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

6.12 การเข้าสู่ระบบสารสนเทศเครือข่ายภายในของสำนักงาน จากผู้ใช้ทั้งที่อยู่ภายนอกและภายในสำนักงาน โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

6.13 IP Address ภายในของระบบสารสนเทศเครือข่ายภายในของสำนักงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถล่วงรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานได้โดยง่าย

6.14 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

6.15 การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์ฯ และผู้ดูแลระบบก่อน และต้องจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

6.16 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น

7. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต และให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ ตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้อง และมีความพร้อมใช้งานอยู่เสมอ ดังนี้

7.1 ผู้ดูแลระบบ (system administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (domain controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของสำนักงาน และกำหนดบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน

7.2 ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติ เพื่อการเข้าใช้งานด้วยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ดังนี้

1) ระบบต้องไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์
2) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง
3) จำกัดการป้อนรหัสผ่าน โดยป้อนรหัสผ่านผิดพลาดได้ไม่เกิน 3 ครั้ง

4) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

7.3 การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) โดยกำหนดให้ผู้ใช้งานเลือกใช้ขั้นตอนในการยืนยันตัวตนที่เหมาะสม มีแนวปฏิบัติ ดังนี้

1) ผู้ใช้งานต้องระบุบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (Password) สำหรับยืนยันตัวตนเพื่อเข้าใช้งานเครื่องคอมพิวเตอร์และระบบสารสนเทศของสำนักงาน

2) การใช้งานบัญชีรายชื่อผู้ใช้งานแบบกลุ่ม ต้องขึ้นอยู่กับความจำเป็นทางด้านการปฏิบัติงานหรือด้านเทคนิค

3) สามารถใช้อุปกรณ์การควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Token key หรือเครื่องอ่านลายนิ้วมือ (finger print) เป็นต้น

7.4 การบริหารจัดการรหัสผ่าน (Password Management System) ต้องมีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกบัญชีชื่อผู้ใช้งานหรือรหัสผ่านของผู้ใช้งานที่ถูกกำหนดไว้ตอนเริ่มต้นที่มาพร้อมกับการติดตั้งระบบทันที

7.5 ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยของสำนักงานที่ได้กำหนดไว้ ให้ดำเนินการดังนี้

1) จำกัดสิทธิการเข้าถึงและกำหนดสิทธิอย่างรัดกุม ในการอนุญาตให้ใช้งานโปรแกรมเป็นรายครั้งไป

2) ห้ามมิให้ลงโปรแกรมอรรถประโยชน์ก่อนได้รับการอนุมัติหรืออนุญาต และยังไม่ผ่านการตรวจสอบ

3) ไม่อนุญาตให้มีการติดตั้งโปรแกรมอรรถประโยชน์ที่เป็นการละเมิดลิขสิทธิ์หรือละเมิดกฎหมายอันจะก่อให้เกิดความเสียหายต่อตนเองและต่อสำนักงาน

4) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

5) ต้องเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

6) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

7.6 กำหนดระยะเวลาการยุติการใช้งานระบบสารสนเทศ (Session Time-Out) เมื่อว่างเว้นจากการใช้งานเป็นเวลา 30 นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบ เมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลา 15 นาที ยกเว้นในระบบที่มีความจำเป็นให้มีระยะเวลาที่นานขึ้น ให้พิจารณาเป็นรายระบบตามความเหมาะสมและจำเป็นเพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต และต้องพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบอีกครั้ง หลังจากระบบได้ตัดการใช้งานนั้นไปแล้ว

7.7 การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลา 1 ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง หากต้องการเชื่อมต่อใหม่ ต้องพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบอีกครั้ง ยกเว้นในระบบที่มีความจำเป็นให้มีระยะเวลาที่นานขึ้น ให้พิจารณาเป็นรายระบบตามความเหมาะสมจำเป็น

8. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

8.1 การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ดังนี้

8.1.1 ผู้ดูแลระบบต้องจัดให้มีการลงทะเบียนผู้ใช้งาน พร้อมทั้งกำหนดสิทธิตามหน้าที่รับผิดชอบ โดยมีผู้บังคับบัญชาเป็นผู้อนุมัติการให้สิทธินั้น และต้องมีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ หรืออย่างน้อยปี ละ 1 ครั้ง

8.1.2 ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อกับระบบงาน (Session Time Out) หากมีการเว้นว่างจากการใช้งานเกินระยะเวลา 30 นาที ต้องทำการยุติการใช้งานทันที

8.1.3 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

1) กำหนดสิทธิให้กับผู้ใช้งานระบบโดยการกำหนดบัญชีชื่อผู้ใช้และรหัสผ่าน เพื่อใช้ในการพิสูจน์ตัวตนของผู้เข้าถึงข้อมูลในแต่ละระดับชั้น

2) การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องมีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น และต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ตามหน้าที่รับผิดชอบของผู้ใช้งาน

3) การนำอุปกรณ์คอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกนอกสำนักงาน กรณีข้อมูลที่เป็นความลับของสำนักงาน ต้องมีการทำลายข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูล

4) การเข้าถึงสารสนเทศจากหน่วยงานภายนอกรวมถึงผู้รับจ้างที่ได้รับมอบหมายเพื่อดำเนินการใดๆ จะต้องได้รับสิทธิและอนุญาตในการเข้าดำเนินการ และจะต้องรายงานให้ทราบหลังจากเสร็จสิ้นแล้ว ผู้ดูแลระบบจะต้องยกเลิกสิทธิที่ให้กับหน่วยงานนั้นๆ ซึ่งหากหน่วยงานภายนอกดำเนินการใดๆ ที่มีผลกระทบต่อระบบ ผู้ดูแลระบบจะต้องเป็นผู้รับผิดชอบ

8.1.4 ต้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ พฤติกรรมการใช้งานการเข้าถึงระบบสารสนเทศที่สำคัญ

8.2 การควบคุมระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน

8.2.1 ต้องแยกระบบซึ่งไวต่อการรบกวนที่มีผลกระทบและมีความสำคัญสูงออกจากระบบอื่นๆ ให้ทำงานอยู่บนเครื่องแม่ข่าย (server) โดยไม่ปะปนกับระบบอื่น เพื่อป้องกันความผิดพลาดอันอาจจะเกิดจากระบบอื่นซึ่งทำงานอยู่บนเครื่องเดียวกัน ซึ่งจำเป็นต้องติดตั้งห้องควบคุมเครื่องแม่ข่ายที่มีสภาพแวดล้อมเหมาะสม

8.2.2 จัดพื้นที่ควบคุมพิเศษ (ห้องควบคุมเครื่องแม่ข่าย) เพื่อควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ ได้แก่ ระบบไฟฟ้า ระบบสำรองไฟฟ้า ระบบควบคุมการเข้าออกพื้นที่ควบคุมพิเศษ หรือทรัพยากรอื่นใด เพื่อป้องกันการหยุดชะงักการทำงานของระบบ

8.2.3 กำหนดค่าที่ไฟร์วอลล์ เพื่อควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอก

8.2.4 มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญ โดยผู้ไม่ได้รับอนุญาต

8.3 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ การปฏิบัติงานจากภายนอกสำนักงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

9. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

9.1 ต้องกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

9.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานต่อผู้อำนวยการศูนย์ฯ โดยทันที

9.3 ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet, ftp หรือ ping เป็นต้น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

9.4 ควรดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

9.5 ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

9.6 การเข้าถึง System Utilities ที่ปฏิบัติการด้วยสิทธิพิเศษในระดับสูง ซึ่งทำให้สามารถเลี่ยงผ่านกลไกการควบคุมระบบ/แอปพลิเคชันต่างๆ ได้นั้น ต้องถูกจำกัดให้เฉพาะผู้ใช้งาน หรือผู้ดูแลระบบ ที่มีความจำเป็นต้องใช้งานเป็นประจำเท่านั้น สำหรับการใช้งานและการเข้าถึง System Utilities เหล่านั้นโดยบุคคลอื่น ให้พิจารณาอนุมัติในลักษณะชั่วคราวในทุกกรณี

9.7 System Utilities ดังกล่าวข้างต้นต้องถูกแยกออกจากแอปพลิเคชัน และซอฟต์แวร์อื่นๆ เพื่อประโยชน์ในการจำกัดการเข้าถึง ให้แก่ผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

9.8 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบเท่านั้น

9.9 ควบคุมการติดตั้งซอฟต์แวร์ไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ โดยผู้ดูแลระบบ ดังนี้

9.9.1 ควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของสำนักงาน เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศ

9.9.2 ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของสำนักงาน

9.9.3 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศ ต้องมีการขออนุมัติจากผู้อำนวยการศูนย์ฯ ก่อนดำเนินการ

9.9.4 ไม่ติดตั้งซอร์สโค้ดคอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

9.9.5 กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย และจำกัดการเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

9.9.6 กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบสารสนเทศ เป็นต้น

9.9.7 วางแผนการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

9.9.8 จัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ที่ไม่ได้ใช้งานไว้อย่างปลอดภัยเพื่ออ้างอิง

9.10 ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลงระบบปฏิบัติการ

9.10.1 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวน ก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

9.10.2 วางแผนเฝ้าระวังและทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

10. การบริหารจัดการการบันทึกและตรวจสอบ

10.1 การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ได้แก่ การบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 3 เดือน โดยมีรายละเอียดการบันทึกพฤติกรรมการใช้งาน (logs) การเข้าถึงระบบสารสนเทศ ดังนี้

1) ข้อมูลบัญชีชื่อผู้ใช้งาน
2) ข้อมูลวัน/เวลาที่เข้าถึงระบบ
3) ข้อมูลวัน/เวลาที่ออกจากระบบ
4) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
5) ข้อมูลการล็อกอิน (Log in) ทั้งที่สำเร็จและไม่สำเร็จ
6) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
7) ข้อมูลการเปลี่ยนการกำหนดค่า (Configuration) ของระบบ
8) ข้อมูลแสดงการใช้งานแอปพลิเคชัน (Application)
9) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น
10) ข้อมูลไอพีแอดเดรส (IP Address) ที่เข้าถึง
11) ข้อมูลโพรโทคอล (Protocol) เครือข่ายที่ใช้
12) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์
13) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

10.2 ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

10.3 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

11. การควบคุมการเข้าใช้งานระบบจากภายนอก

ศูนย์ฯ ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายใน เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

11.1 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของสำนักงาน การควบคุมบุคคลที่เข้าสู่ระบบของสำนักงานจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

11.2 วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์ฯ ก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

11.3 ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสำนักงานอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

11.4 ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้าองค์การนั้น ต้องดูและการจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

11.5 การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

12. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

12.1 ผู้ใช้งานระบบสารสนเทศทุกคน เมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบของสำนักงาน สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

12.1.1 การแสดงตัวตน (Identification) คือ ขั้นตอนที่ผู้ใช้แสดงบัญชีชื่อผู้ใช้งาน (Username)

12.1.2 การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ดหรือการใช้ USB Token ที่มีเทคโนโลยี Public Key Infrastructure: PKI ด้วยการลงลายมือชื่อดิจิทัล (Digital Signature) และการเข้ารหัสลับ (Encryption) รูปแบบของใบรับรองอิเล็กทรอนิกส์ เป็นต้น

12.2 การเข้าสู่ระบบสารสนเทศของสำนักงานนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย 1 วิธี

12.3 การเข้าสู่ระบบสารสนเทศของสำนักงานจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบผู้ใช้งานด้วย

12.4 การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

13. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

เพื่อปกป้องระบบสารสนเทศจากการปฏิบัติงานจากภายนอกสำนักงาน กำหนดแนวปฏิบัติเพื่อความมั่นคงปลอดภัย ดังนี้

13.1 การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ต้องมีการเข้ารหัส (Encryption) ด้วยวิธีการ SSL VPN หรือ XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากลในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกสำนักงานและระบบงานต่างๆ ภายในสำนักงาน

13.2 การเข้าถึงระบบสารสนเทศของสำนักงานจากระยะไกล ด้วยอุปกรณ์ที่เป็นของส่วนตัว ต้องได้รับอนุญาตจาก ผู้อำนวยการศูนย์ฯ

13.3 การเข้าสู่ระบบระบบสารสนเทศในสำนักงานจากระยะไกล ต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยบัญชีชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

13.4 ผู้ได้รับอนุญาตเท่านั้นจึงจะสามารถเข้าถึงระบบสารสนเทศและข้อมูลของสำนักงาน โดยไม่ให้สมาชิกภายในครอบครัวหรือบุคคลอื่นใดสามารถเข้าถึงระบบได้

13.5 ผู้ดูแลระบบต้องควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และมีการเฝ้าระวังสม่ำเสมอ เมื่อพบเหตุการณ์ผิดปกติต้องระงับการให้บริการทันที

13.6 ผู้ดูแลระบบจะทำการยกเลิกสิทธิการเข้าถึงระบบสารสนเทศในการปฏิบัติงานภายนอกสำนักงาน แก่ผู้ใช้งานทันทีเมื่อครบกำหนดระยะเวลาขออนุญาต หรือมีหนังสือเป็นลายลักษณ์อักษรเพื่อขอยกเลิกต่อผู้อำนวยการศูนย์ฯ

13.7 ผู้ดูแลระบบต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศจากการปฏิบัติงานภายนอกสำนักงานอย่างน้อยปีละ 1 ครั้ง

หมวด 4 การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third party access control)

1. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอก อาจก่อให้เกิดความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก

2. แนวทางปฏิบัติ

2.1 ต้องมีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรืออุปกรณ์ที่ใช้ในการประมวลผล โดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสม ก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

2.2 การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

2.2.1 บุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการศูนย์ฯ

2.2.2 จัดทำเอกสารแบบฟอร์มสำหรับหน่วยงานภายนอก เพื่อระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

1) เหตุผลในการขอใช้
2) ระยะเวลาในการใช้
3) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย
4) การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ
5) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

2.2.3 หน่วยงานภายนอกที่ปฏิบัติงานให้กับสำนักงาน ไม่ว่าจะทำงานอยู่ภายในหรือภายนอกสำนักงาน จำเป็นต้องลงนามในสัญญาไม่เปิดเผยข้อมูลของสำนักงาน โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศของสำนักงาน

2.2.4 สำนักงาน ควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เข้าไปปฏิบัติงาน

2.2.5 เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

2.2.6 สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของสำนักงาน ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความมั่นคงปลอดภัย ทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

2.2.7 สำนักงานมีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มั่นใจว่าสำนักงานสามารถควบคุมการใช้งานได้อย่างทั่วถึง ตามสัญญานั้น

2.2.8 ควรดำเนินการให้ผู้ให้บริการภายนอก จัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

2.3 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

2.3.1 กำหนดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์ โดยผู้ให้บริการภายนอก

2.3.2 ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก

2.3.3 กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก รวมถึงข้อตกลงในการรักษาความลับ โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

2.3.4 กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ก่อนการติดตั้ง

2.3.5 การทดสอบซอฟต์แวร์ ห้ามทดสอบบนระบบและฐานข้อมูลที่ใช้งาน ต้องสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบ เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งาน

2.4 มาตรการควบคุมผู้ให้บริการภายนอก (Outsource)

2.4.1 ผู้ให้บริการภายนอกที่ต้องการสิทธิในการเข้าถึงระบบสารสนเทศของสำนักงาน จะต้องเป็นผู้ให้บริการที่ผ่านกระบวนการจัดซื้อจัดจ้าง และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการศูนย์ฯ

2.4.2 ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอกที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้

2.4.3 กำหนดให้ผู้ให้บริการภายนอกเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น ทั้งนี้ หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการภายนอกอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

2.4.4 การอนุญาตให้ผู้ให้บริการภายนอกเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้นและไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้

ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าว ต้องมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจากผู้อำนวยการศูนย์ฯ ก่อนทุกครั้ง

2.5 มาตรการควบคุมช่องโหว่ทางเทคนิค

2.5.1 การบริหารจัดการช่องโหว่ของระบบ ควรมีการบันทึกดังต่อไปนี้

1) ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
2) สถานที่ที่ติดตั้ง
3) เครื่องแม่ข่ายที่ติดตั้ง
4) ผู้ผลิตซอฟต์แวร์
5) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้นๆ

2.5.2 กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

2.5.3 กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบดำเนินการ ดังนี้

1) มีการเฝ้าระวังและติดตามประเมินความเสี่ยง สำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงาน เพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
2) ให้กำหนดแหล่งข้อมูลข่าวสาร เพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของสำนักงาน
3) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยง เมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

2.5.4 ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

หมวด 5 การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
(Use of Personal Computer)

1. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และผู้ใช้งานควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของสำนักงาน ให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

2. การใช้งานทั่วไป

2.1 เครื่องคอมพิวเตอร์ส่วนบุคคลที่สำนักงานอนุญาตให้เจ้าหน้าที่ใช้งาน เป็นทรัพย์สินของสำนักงาน เพื่อใช้ในงานราชการ ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ เพื่อประโยชน์ของสำนักงาน

2.2 เครื่องคอมพิวเตอร์ส่วนบุคคลของสำนักงาน ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยอยู่ในความรับผิดชอบของหน่วยงานภายใน ผู้ใช้งานต้องได้รับอนุญาตจากผู้บังคับบัญชาของหน่วยงานภายในก่อนใช้งานเครื่องคอมพิวเตอร์นั้น และผู้ดูแลครุภัณฑ์ของหน่วยงานภายในจะต้องระบุว่าผู้ใดเป็นผู้ครอบครองเครื่องคอมพิวเตอร์นั้น

2.3 เจ้าหน้าที่ศูนย์ฯ เป็นผู้ทำการติดตั้งโปรแกรมพื้นฐานและระบบปฏิบัติการลงบนเครื่องคอมพิวเตอร์ รวมถึงกำหนดชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคล ทั้งนี้ ต้องเป็นผู้ที่ผู้อำนวยการศูนย์ฯ มอบหมายให้ทำหน้าที่เป็นผู้ติดตั้งโปรแกรมและระบบปฏิบัติการเท่านั้น

2.4 โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ของสำนักงาน ต้องเป็นโปรแกรมที่สำนักงานซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.5 ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของสำนักงาน หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหาย หรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

2.6 การเคลื่อนย้ายเครื่องคอมพิวเตอร์ส่วนบุคคลออกนอกพื้นที่ปฏิบัติงานของหน่วยงานภายในจะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา และแจ้งให้ผู้ดูแลครุภัณฑ์ทราบก่อนนำออกนอกสถานที่

2.7 การนำเครื่องคอมพิวเตอร์ส่วนบุคคลของสำนักงานส่งซ่อมภายนอก จะต้องผ่านการตรวจประเมินจากเจ้าหน้าที่ศูนย์ฯ ที่ผู้อำนวยการศูนย์ฯ มอบหมายให้ปฏิบัติหน้าที่ซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ก่อน หากเห็นสมควรส่งซ่อมภายนอกต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์ฯ โดยการเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม จะต้องดำเนินการโดยเจ้าหน้าที่

ศูนย์ฯ หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญาไว้กับทางสำนักงานเท่านั้น

2.8 ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบหาไวรัส โดยโปรแกรมป้องกันไวรัส

2.9 ไม่ควรเก็บข้อมูลสำคัญของสำนักงานไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

2.10 ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของสำนักงาน

2.11 ผู้ใช้งานมีหน้าที่รับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยหลีกเลี่ยงการวางอาหารหรือเครื่องดื่มบริเวณเครื่องคอมพิวเตอร์ และไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

3. การควบคุมการเข้าถึงระบบปฏิบัติการ

3.1 ผู้ใช้งานต้องยืนยันตัวตนด้วยบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน

3.2 ผู้ใช้งานควรกำหนดรหัสผ่านที่มีคุณภาพตามคุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี

3.3 ผู้ใช้งานต้องตั้งค่าการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 10 นาที และต้องใส่รหัสผ่านให้ถูกต้องเมื่อต้องการใช้งาน

3.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

3.5 ผู้ใช้ต้องทำการลงบันทึกออก (Logout) จากระบบทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

4. แนวทางปฏิบัติในการใช้รหัสผ่าน

4.1 ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร "การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

5. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

5.1 ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ และเป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

5.2 เจ้าหน้าที่ศูนย์ฯ มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์เป็นโปรแกรมพื้นฐาน

5.3 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ส่วนบุคคล และผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Thumb Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

5.4 ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

5.5 ผู้ใช้งานต้องตรวจสอบว่าข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

6. การสำรองข้อมูลและการกู้คืน

6.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เพื่อป้องกันการสูญหายของข้อมูล

6.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

6.3 ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Data Storage ไม่ควรเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

หมวด 6 การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
(Use of Notebook Computer)

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพา และการนำไปปฏิบัติงานภายนอกสำนักงาน และเป็นการป้องกันทรัพยากรและข้อมูลที่มีค่าของสำนักงานให้เกิดความปลอดภัย ผู้ใช้งานจึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ควรหลีกเลี่ยงในการใช้งานเครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

2. การใช้งานทั่วไป

2.1 เครื่องคอมพิวเตอร์แบบพกพาที่สำนักงานอนุญาตให้เจ้าหน้าที่ใช้งาน เป็นทรัพย์สินของสำนักงานเพื่อใช้ในงานราชการ ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่อประโยชน์ของสำนักงาน

2.2 เครื่องคอมพิวเตอร์แบบพกพาของสำนักงาน ขึ้นทะเบียนและควบคุมด้วยหมายเลขครุภัณฑ์ โดยอยู่ในความรับผิดชอบของหน่วยงานภายใน ผู้ใช้งานต้องได้รับอนุญาตจากผู้บังคับบัญชาของหน่วยงานภายในก่อนใช้งานเครื่องคอมพิวเตอร์นั้น และผู้ดูแลครุภัณฑ์ของหน่วยงานภายในจะต้องระบุว่าผู้ใดเป็นผู้ครอบครองหรือนำไปใช้งาน

2.3 เจ้าหน้าที่ศูนย์ฯ เป็นผู้ทำการติดตั้งโปรแกรมพื้นฐานและระบบปฏิบัติการลงบนเครื่องคอมพิวเตอร์ รวมถึงกำหนดชื่อเครื่องคอมพิวเตอร์ (Computer name) แบบพกพา ทั้งนี้ ต้องเป็นผู้ที่ผู้อำนวยการศูนย์ฯ มอบหมายให้ทำหน้าที่เป็นผู้ติดตั้งโปรแกรมและระบบปฏิบัติการเท่านั้น

2.4 โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ของสำนักงาน ต้องเป็นโปรแกรมที่สำนักงานซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

2.5 ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งหรือแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์แบบพกพาของสำนักงาน หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหาย หรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงผู้เดียว

2.6 การนำเครื่องคอมพิวเตอร์แบบพกพาของสำนักงานไปใช้งานภายนอกพื้นที่ปฏิบัติงานของหน่วยงานภายใน จะต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา และแจ้งให้ผู้ดูแลครุภัณฑ์ทราบก่อนนำออกนอกสถานที่

2.7 การนำเครื่องคอมพิวเตอร์แบบพกพาของสำนักงานส่งซ่อมภายนอก จะต้องผ่านการตรวจประเมินจากเจ้าหน้าที่ศูนย์ฯ ที่ผู้อำนวยการศูนย์ฯ มอบหมายให้ปฏิบัติหน้าที่ซ่อมบำรุงอุปกรณ์คอมพิวเตอร์ก่อน หากเห็นสมควรส่งซ่อมภายนอกต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์ฯ โดยการเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม จะต้องดำเนินการโดยเจ้าหน้าที่

ศูนย์ฯ หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญาไว้กับทางสำนักงานเท่านั้น

2.8 การเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรจัดเก็บเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ใส่ในกระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาให้เรียบร้อย เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน การหลงลืมอุปกรณ์ และไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาในกระเป๋าเดินทางที่เสี่ยงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่อง หรืออาจถูกจับโยนได้

2.9 กรณีที่ต้องการเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้นโดยเด็ดขาด

2.10 ห้ามมิให้ผู้ใช้ทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่ และควรรักษาสภาพคอมพิวเตอร์ให้มีสภาพพร้อมใช้งานตลอดเวลา

2.11 ผู้ใช้ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

2.12 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

2.13 ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์

2.14 การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่าเบามือที่สุด และควรเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจำทำให้หน้าจอมีรอยขีดข่วนได้

3. ความปลอดภัยทางด้านกายภาพ

3.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย ดังนั้น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

3.2 การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์ เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

3.3 ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพา ในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

3.4 ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่างๆ เป็นต้น

3.5 ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน

3.6 ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

4. การควบคุมการเข้าถึงระบบปฏิบัติการ

4.1 ผู้ใช้งานต้องยืนยันตัวตนด้วยบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพาของสำนักงาน

4.2 ผู้ใช้งานควรกำหนดรหัสผ่านที่มีคุณภาพตามคุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี

4.3 ผู้ใช้งานต้องตั้งค่าการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นระยะเวลา 10 นาที และต้องใส่รหัสผ่านให้ถูกต้องเมื่อต้องการใช้งาน

4.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้บัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

4.5 ผู้ใช้ต้องทำการ Logout จากระบบทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

5. แนวทางปฏิบัติในการใช้รหัสผ่าน

5.1 ให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

6. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

6.1 ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมใช้งานต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ และเป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

6.2 เจ้าหน้าที่ศูนย์ฯ มีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์เป็นโปรแกรมพื้นฐาน

6.3 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัส ที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา และผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Thumb Drive และ Data Storage อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

6.4 ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

6.5 หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่นๆ ได้

7. การสำรองข้อมูลและการกู้คืน

7.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาไว้บนสื่อบันทึกอื่นๆ เพื่อป้องกันการสูญหายของข้อมูล

7.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

7.3 ผู้ใช้ควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้ใน Data Storage ไม่ควรเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

7.4 แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก

หมวด 7 การใช้งานอินเทอร์เน็ต และเครือข่ายสังคมออนไลน์
(Use of the Internet and Social Network)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์แนวทางปฏิบัติ ในการใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์อย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ได้แก่ การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่น อันก่อให้เกิดการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของสำนักงานถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

2.1 ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่สำนักงานจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IP-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการศูนย์ฯ เป็นลายลักษณ์อักษรแล้ว

2.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่

2.3 การรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต จะต้องมีการตรวจสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัส ก่อนการรับส่งข้อมูลทุกครั้ง

2.4 ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของสำนักงานนอกเหนือจากเพื่อประโยชน์ของทางราชการ หรือทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เว้นแต่เป็นการดำเนินงานตามภารกิจของสำนักงาน

2.5 ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของสำนักงาน

2.6 ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว หรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับสำนักงาน

2.7 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงาน ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

2.8 ผู้ใช้งานต้องไม่นำเข้าข้อมูลคอมพิวเตอร์คอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

2.9 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด อันจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

2.10 ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

2.11 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่างๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

2.12 การใช้งานเว็บบอร์ด (Web Board) ของสำนักงาน ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสำนักงาน

2.13 ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงาน การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่นๆ

2.14 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ต้องปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

3. แนวทางปฏิบัติในการใช้งานเครือข่ายสังคมออนไลน์

3.1 อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่สำนักงานได้กำหนดไว้เท่านั้น เช่น Facebook , Line , Twitter

3.2 หากต้องการใช้งานเครือข่ายสังคมออนไลน์ในลักษณะอื่นใดนอกเหนือจากที่สำนักงานกำหนดให้ขออนุญาตจากผู้อำนวยการศูนย์ฯ ก่อนใช้งาน

3.3 ผู้ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักในเรื่องความมั่นคงปลอดภัยอยู่เสมอ ต้องไม่เปิดเผยข้อมูลที่สำคัญ ข้อมูลเฉพาะส่วนตัว หรือข้อมูลความลับของสำนักงาน

3.4 ผู้ใช้งานพึงตระหนักว่าข้อความหรือความเห็นที่เผยแพร่บนเครือข่ายสังคมออนไลน์ เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ในการใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุ ให้ร้าย ยุยง ท้าทาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง พึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง

3.5 ผู้ใช้งานพึงตระหนักว่าพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะ ไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลที่มีการรายงานจะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้จะเป็นการแสดงความคิดเห็นในนามบัญชีชื่อผู้ใช้ส่วนตัว แต่อาจส่งผลกระทบกับสำนักงานได้ และพึงระมัดระวังเรื่องผลประโยชน์ในเชิงพาณิชย์

3.6 หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ที่อาจมีผลกระทบต่อสำนักงาน ผู้ใช้งานต้องแจ้งต่อผู้อำนวยการศูนย์ฯ โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

3.7 ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

หมวด 8 การใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

1. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของสำนักงาน ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้น จากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด อันจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

2.1 ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน ให้เหมาะสมกับหน้าที่และความรับผิดชอบของผู้ใช้งาน โดยผู้ใช้งานต้องกรอกแบบฟอร์มการขอใช้งานระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน และให้ผู้บังคับบัญชาลงนามอนุมัติเพื่อรับรองข้อมูลและพิจารณาเหตุผลความจำเป็น

2.2 ผู้ดูแลระบบต้องมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง การโอน ย้าย ลาออก หรือสิ้นสุดสัญญาจ้าง

2.3 ผู้ดูแลระบบกำหนดบัญชีชื่อผู้ใช้งาน E-Mail (username) และรหัสผ่าน (password) สำหรับการใช้งานครั้งแรก ให้แก่ผู้ใช้งาน โดยส่งมอบให้ผู้ใช้งานเป็นเอกสารปิดผนึกที่เป็นความลับ หรือทางอีเมลส่วนบุคคลของผู้ใช้งาน

2.4 ผู้ใช้งานต้องเปลี่ยนรหัสผ่านใหม่ทันทีเมื่อได้รับรหัสผ่านครั้งแรก (Default Password) หรือเมื่อเข้าระบบครั้งแรก ระบบจะต้องบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ และควรเปลี่ยนรหัสผ่านใหม่ทุก 6 เดือน

2.5 การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”

2.6 ระบบต้องไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งาน ระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านต้องแสดงด้วยรูปแบบของสัญลักษณ์แทนตัวอักษร เช่น ‘x’ หรือ ‘*’ ในการพิมพ์แต่ละตัวอักษร

2.7 ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดได้ ซึ่งในทางปฏิบัติโดยทั่วไปไม่เกิน 3 ครั้ง หากเกินกว่าที่กำหนดระบบจะทำการล็อคสิทธิการเข้าถึงของผู้ใช้งานทำให้ไม่สามารถใช้งานได้จนกว่าผู้ดูแลระบบจะปลดล็อคให้

2.8 ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ออกจากระบบโดยอัตโนมัติ (Time out) เพื่อตัดการใช้งานระบบ เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลา 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องยืนยันตัวตนด้วยบัญชีชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

2.9 ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

2.10 ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อสำนักงาน หรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของสำนักงาน

2.11 ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่น เพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของแล้วเท่านั้น และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

2.12 ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของสำนักงาน เพื่อการทำงานของสำนักงานเท่านั้น

2.13 หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการ Logout ออกจากระบบ และปิดเว็บเบราว์เซอร์ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต

2.14 ผู้ใช้ต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด ด้วยโปรแกรมป้องกันไวรัส เป็นการป้องกันการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น

2.15 ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

2.16 ผู้ใช้งานต้องใช้คำที่สุภาพในการส่งจดหมายอิเล็กทรอนิกส์ และใช้ความระมัดระวังในการระบุชื่อที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้รับให้ถูกต้อง และระบุชื่อของผู้ส่งในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งไป รวมทั้งจำกัดกลุ่มผู้รับจดหมายอิเล็กทรอนิกส์เท่าที่มีความจำเป็นต้องรับรู้รับทราบ

2.17 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

2.18 ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (Inbox) ของตนเองทุกวัน และควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์ให้เหลือจำนวนน้อยที่สุด

2.19 ผู้ใช้งานควรทำการสำรองข้อมูลจดหมายอิเล็กทรอนิกส์ที่สำคัญ ตามความจำเป็นอย่างสม่ำเสมอ

2.20 ข้อควรระวัง ผู้ใช้งานไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

2.21 ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบในการเก็บรักษาบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) เป็นความลับไม่ให้บุคคลอื่นล่วงรู้

หมวด 9 การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการในการควบคุม ป้องกัน และการรักษาความปลอดภัยการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของสำนักงาน เพื่อป้องกันและรักษาความปลอดภัยของข้อมูลสารสนเทศของสำนักงาน

2. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

2.1 ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของสำนักงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาหรือผู้อำนวยการศูนย์ฯ ก่อนเท่านั้น

2.2 ผู้ดูแลระบบ กำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่และความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.3 ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

2.4 ผู้ดูและระบบต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณ (Access Point: AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

2.5 ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ ทั้งนี้ การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

2.6 ผู้ดูแลระบบต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

2.7 ผู้ดูแลระบบต้องเปลี่ยนค่า ชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

2.8 ผู้ดูแลระบบต้องกำหนดค่าใช้มาตรฐานความปลอดภัยแบบ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ เพื่อให้ยากต่อการดักจับ ช่วยให้ปลอดภัยมากขึ้น

2.9 ผู้ดูแลระบบต้องเลือกใช้วิธีการควบคุม MAC Address ร่วมกับบัญชีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address บัญชีชื่อผู้ใช้งาน และรหัสผ่านตามที่กำหนดไว้เท่านั้น ในการเชื่อมต่อกับเครือข่ายไร้สายตาม SSID ที่กำหนดไว้ สำหรับบุคคลภายนอก

กำหนดให้ใช้งานเครือข่ายไร้สายโดยไม่ควบคุม MAC Address แต่ให้ใช้งานได้ตาม SSID ที่ผู้ดูแลระบบกำหนดแยกเฉพาะสำหรับบุคคลภายนอกเท่านั้น

2.10 ผู้ดูแลระบบต้องมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในสำนักงาน

2.11 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานในระบบเครือข่ายไร้สาย ติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

2.12 ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

หมวด 10 การใช้งานระบบไฟร์วอลล์
(Firewall Policy)

1. วัตถุประสงค์

เพื่อป้องกันการบุกรุกจากบุคคลภายนอกในการเข้าถึงระบบเครือข่ายภายในของสำนักงาน และทำการตรวจสอบติดตามแพ็คเก็ต (Packet) โดยจะอนุญาตให้ผู้มีสิทธิเข้าออกระบบ เพื่อควบคุมการเชื่อมต่อจากภายนอกสู่ภายในสำนักงาน และจากภายในสำนักงานสู่ภายนอกสำนักงาน

2. แนวทางปฏิบัติในการรักษาความปลอดภัยไฟร์วอลล์ (Firewall)

2.1 ผู้ดูแลระบบต้องเฝ้าระวังและบริหารจัดการระบบรักษาความปลอดภัย (Firewall)

2.2 ผู้ดูแลระบบต้องกำหนดนโยบาย (Policy) การใช้งานไฟร์วอลล์

2.3 ผู้ดูแลระบบต้องจัดให้มีระบบตรวจสอบยืนยันตัวตนและสิทธิการเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ

2.4 ผู้ดูแลระบบต้องกำหนดค่า (Configuration) หรือกำหนดนโยบาย (Policy) เพื่อกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ป้องกันผู้บุกรุก ไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์

2.5 ผู้ดูแลระบบต้องกำหนดขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติต้องดำเนินการแก้ไข รวมทั้งมีการรายงานผู้อำนวยการศูนย์ฯ โดยทันที

2.6 การเปิดใช้บริการ (Service) ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์ฯ ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ผู้ดูแลระบบต้องกำหนดมาตรการป้องกันเพิ่มเติม

2.7 ผู้ดูแลระบบต้องบริหารจัดการให้ไฟร์วอลล์สามารถเปิดใช้งานได้ตลอดเวลา และในกรณีที่พบปัญหาหรือการทำงานในลักษณะที่ผิดปกติต้องดำเนินการแก้ไข รวมทั้งมีการรายงานผู้อำนวยการศูนย์ฯ โดยทันที

2.8 ผู้ดูแลระบบต้องออกจากระบบ (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์

2.9 ผู้ดูแลระบบต้องกำหนดให้มีการควบคุมการใช้งาน โดยบริหารจัดการบัญชีรายชื่อผู้ใช้งาน

2.10 ผู้ดูแลระบบต้องบันทึกบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อยืนยันตัวตนผู้ใช้งานก่อนเข้าใช้งานระบบ (Authentication) และควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไข เปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง

2.11 ผู้ดูแลระบบต้องติดตั้ง Patch ที่จำเป็นของระบบงานสำคัญ เพื่ออุดช่องโหว่ต่างๆ ของซอฟต์แวร์ระบบ (System Software)

2.12 ผู้ดูแลระบบต้องทดสอบซอฟต์แวร์ระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังการแก้ไข หรือบำรุงรักษา

2.13 ผู้อำนวยการศูนย์ฯ ต้องกำหนดผู้รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ อย่างชัดเจน

2.14 ผู้ขอใช้งานต้องยอมรับและปฏิบัติตามนโยบายด้านความปลอดภัยอย่างเคร่งครัด

2.15 ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบ ของสำนักงาน หรือกฎหมาย หรืออาจจะทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศ จะยกเลิกการให้บริการทันที

หมวด 11 การใช้งานระบบตรวจจับและป้องกันผู้บุกรุก
(Intrusion Detection System (IDS) and Intrusion Prevention System (IPS))

1. วัตถุประสงค์

เพื่อป้องการบุกรุกจากบุคคลที่ไม่พึงประสงค์ โดยมีรายงานที่สามารถตรวจสอบการดำเนินกิจกรรมของผู้ใช้งานได้ ตลอดจน ติดตามสืบค้นหาช่องโหว่ของระบบ และค้นหาที่มาของผู้บุกรุกได้อย่างมีประสิทธิภาพ

2. แนวทางปฏิบัติในการใช้งานระบบตรวจจับและป้องกันผู้บุกรุก

2.1 ผู้ดูแลระบบต้องกำหนดให้มีการเฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ (IDS/IPS) เหตุการณ์ผิดปกติ และการแจ้งเตือนต่างๆ ที่อุปกรณ์ตรวจพบ จะถูกทำการวิเคราะห์และหาสาเหตุของการบุกรุกในระบบเทคโนโลยีสารสนเทศของสำนักงาน เพื่อเป็นเครื่องมือสำหรับการสืบสวนหาบุคคลที่โจมตี บุกรุก หรือใช้ระบบในทางที่ผิด และเป็นการป้องกันก่อนที่จะเกิดการโจมตี

2.2 ผู้ดูแลระบบต้องเก็บสถิติเกี่ยวกับความพยายามบุกรุกหรือโจมตีสำนักงาน เป็นเครื่องมือวัดประสิทธิภาพในการป้องกันภัยของระบบรักษาความปลอดภัยอื่น เช่น ไฟร์วอลล์ เป็นต้น และเพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ภายในจากอันตรายที่มาจากเครือข่ายคอมพิวเตอร์ภายนอก เช่น ผู้บุกรุก หรือ Hacker รวมทั้งไวรัสประเภทต่างๆ

2.3 ผู้ดูแลระบบต้องมีการบริหารจัดการเหตุการณ์บุกรุกระบบ (Incident Management) เป็นการตอบสนองต่อเหตุการณ์บุกรุกทางเครือข่าย สามารถช่วยวิเคราะห์ลักษณะการบุกรุกทางเครือข่าย และทำให้สามารถแก้ไขสถานการณ์ได้อย่างถูกต้อง ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการบุกรุก โดยต้องจัดลำดับความสำคัญของการบุกรุกจากผลกระทบที่เกิดขึ้นกับสำนักงาน และจัดทำวิธีปฏิบัติที่ถูกต้องให้กับสำนักงานเพื่อป้องกันเหตุการณ์เกิดซ้ำ การตอบสนองต่อเหตุการณ์การบุกรุกแบ่งเป็น 4 ขั้นตอนคือ

2.3.1 จำกัดขอบเขต (Containment) จำกัดพื้นที่ที่เสี่ยงต่อการบุกรุกและจำกัดความรุนแรงของการบุกรุก

2.3.2 กำจัดต้นเหตุ (Eradication) กำจัดต้นเหตุของการบุกรุก รวมถึงปิดกั้นช่องทางของการบุกรุก

2.3.3 กู้คืนระบบ (Recovery) แก้ไขระบบที่ถูกบุกรุกให้สามารถกลับมาทำงานได้ตามปกติ

2.3.4 ติดตามผล (Follow-Up) บันทึกผลกระทบของเหตุการณ์และแนะนำวิธีปฏิบัติเพื่อป้องกันเหตุการณ์เกิดซ้ำ

2.4 ผู้อำนวยการศูนย์ฯ ต้องกำหนดผู้รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆ ของระบบเครือข่าย และอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง

2.5 การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบ

2.6 การใช้เครื่องมือต่างๆ (tools) เพื่อตรวจเช็คระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์ฯ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

2.7 ผู้ดูแลระบบต้องทำการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ และต้องประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (operation) ระบบรักษาความปลอดภัย (security) และการทำงาน (functionality) ของระบบงานที่เกี่ยวข้อง

หมวด 12 การรักษาสภาพความพร้อมใช้งานของการให้บริการ (IT Service Continuity)

1. วัตถุประสงค์

เพื่อมั่นใจได้ว่าระบบสารสนเทศที่ให้บริการและข้อมูลสำคัญของสำนักงาน มีความพร้อมใช้งานอยู่ตลอดและสามารถดำเนินการต่อไปได้ในขณะที่สำนักงานเผชิญกับภาวะวิกฤตหรือภัยพิบัติ เพื่อลดผลกระทบที่อาจเกิดขึ้นกับสำนักงาน โดยมีการลำดับความสำคัญจากผลกระทบจากความเสียหายของทรัพย์สิน และผลการวิเคราะห์ความเสี่ยงเพื่อใช้ในการพิจารณาวิธีการสร้างความต่อเนื่อง

2. แนวทางปฏิบัติในการสำรองข้อมูล ระบบสำรอง และการปฏิบัติงานในสภาวะฉุกเฉิน

2.1 เครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่มีความสำคัญ ต้องมีการสำรองข้อมูลให้อยู่ในสภาพพร้อมใช้งาน

2.2 ผู้ดูแลระบบต้องสำรองข้อมูลและซอฟต์แวร์เก็บไว้ โดยคัดเลือกและจัดเรียงลำดับตามผลกระทบจากความสูญเสียของระบบ ที่มีผลต่อภารกิจหลักของสำนักงาน

2.3 ต้องมีขั้นตอนการปฏิบัติ การสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

2.4 ผู้ดูแลระบบต้องจัดเก็บข้อมูลที่สำรองในสื่อบันทึกข้อมูลสำรอง โดยมีการแสดงชื่อระบบที่สำรอง วัน เดือน ปี และเวลาในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองต้องจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ในสถานที่จัดทำระบบสำรอง (สมช. อาคารศูนย์ราชการฯ แจ้งวัฒนะ) และต้องมีการทดสอบสื่อบันทึกข้อมูลสำรองอย่างสม่ำเสมอ หรืออย่างน้อยปีละ 1 ครั้ง

2.5 ศูนย์ฯ ต้องกำหนดสถานที่และเตรียมพื้นที่ให้อยู่ในสภาพพร้อมใช้งานระบบสำรอง

2.6 ผู้อำนวยการศูนย์ฯ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมฉุกเฉิน

2.7 ศูนย์ฯ ต้องดำเนินการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินปีละ 1 ครั้ง

2.8 ผู้ดูแลระบบต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยระบบสารสนเทศได้ตามปกติ โดยต้องทบทวนแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวอย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

2.9 ศูนย์ฯ และหน่วยงานภายในที่เกี่ยวข้อง ต้องทดสอบปฏิบัติตามคู่มือแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ 1 ครั้ง

หมวด 13 การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(IT Risk Management)

1. วัตถุประสงค์

เพื่อกำหนดกฎเกณฑ์การตรวจสอบและประเมินความเสี่ยงของระบบเครือข่าย และระบบเทคโนโลยีสารสนเทศของสำนักงาน ให้มั่นใจได้ว่าความเสี่ยงของระบบสารสนเทศของสำนักงาน ได้ถูกพิจารณาและได้มีการจัดเตรียมมาตรการในการควบคุมความเสี่ยงที่เหมาะสม เพื่อป้องกันและลดความเสี่ยงด้านความมั่นคงปลอดภัยที่อาจจะเกิดขึ้นกับสำนักงานได้

2. แนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

2.1 การระบุความเสี่ยงให้สอดคล้องกับความเสี่ยงที่อาจจะเกิดขึ้นจริงกับการทำงาน ดังนี้

2.1.1 ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการ เพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

2.1.2 ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

2.1.3 ความเสี่ยงที่เกิดจากเครื่องมือสารสนเทศหรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

2.1.4 ความเสี่ยงที่เกิดจากการลงบันทึกเข้าใช้งาน (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่าย ที่มีบัญชีชื่อผู้ใช้งาน (Username) เดียวกันในเวลาเดียวกันมากกว่าหนึ่งจุด

2.1.5 ความเสี่ยงอื่นที่เกี่ยวข้องกับระบบสารสนเทศสำนักงาน ที่อาจจะส่งผลกระทบกับการปฏิบัติงานของสำนักงานในอนาคต

2.2 การตรวจสอบและประเมินความเสี่ยง ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

2.2.1 ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ ทำการประเมินในแต่ละด้านของผลกระทบ โดยให้พิจารณาถึงมาตรการควบคุมที่มีอยู่ในปัจจุบันด้วย

2.2.2 ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ รวมถึงความเป็นไปได้ที่จะเกิดขึ้น โดยต้องพิจารณา 2 ปัจจัยหลัก ดังนี้ แนวโน้มการเกิดขึ้นของเหตุการณ์ความเสี่ยง พิจารณาจากความน่าจะเป็นหรือค่าทางสถิติที่มีการบันทึกไว้ เช่น เหตุการณ์ความเสี่ยงประเภทภัยธรรมชาติต่างๆ น่าจะมีแนวโน้มการเกิดต่ำ เมื่อดูจากสถิติที่เคยเกิดขึ้น ความยากง่ายที่จะถูกกระทำ พิจารณาจากจุดอ่อนหรือข้อบกพร่องที่มีอยู่ และตัวควบคุมในปัจจุบัน หากมีจุดอ่อนหรือข้อบกพร่องมากและไม่มีตัวควบคุมเลย โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงจะสูงกว่าในกรณีที่มีตัวควบคุมอยู่

2.2.3 จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ พิจารณาข้อบกพร่องของระบบหรือข้อบกพร่องของการควบคุมที่ปัจจุบันอาจจะไม่มีอยู่ และจะส่งผลให้ระบบไม่มีความมั่นคงปลอดภัยที่ดี

2.2.4 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศของสำนักงานอย่างน้อยปีละ 1 ครั้ง

2.2.5 การตรวจสอบจะต้องดำเนินการโดยผู้ตรวจสอบสารสนเทศของสำนักงาน (Internal IT Auditor) อย่างน้อยปีละ 1 ครั้ง

หมวด 14 หน้าที่และความรับผิดชอบด้านสารสนเทศ

1. วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารระดับสูงสุด (CEO) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) ผู้อำนวยการศูนย์ฯ ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่และผู้ใช้งาน

2. แนวทางปฏิบัติ

ส่วนที่ 1 ระดับนโยบาย

1.1 เลขาธิการสภาความมั่นคงแห่งชาติ ในฐานะผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) ของสำนักงาน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่สำนักงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.2 ผู้บริหารที่ปฏิบัติหน้าที่เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (Department Chief Information Officer : DCIO) ของสำนักงาน เป็นผู้รับผิดชอบในการสั่งการ กำกับนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม ดูแล และควบคุมตรวจสอบการดำเนินงานด้านเทคโนโลยีสารสนเทศ ให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.3 ผู้อำนวยการศูนย์ฯ ของสำนักงาน เป็นผู้รับผิดชอบ ดังนี้

1.3.1 กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

1.3.2 ควบคุม ดูแล รักษาความปลอดภัยระบบสารสนเทศและระบบฐานข้อมูล

1.3.3 วางแผน จัดทำ ทบทวน ติดตาม กำกับ ดูแล แผนสำรอง และแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ส่วนที่ 2 ระดับปฏิบัติงาน

ระดับผู้ปฏิบัติงานประกอบด้วย ผู้ดูแลระบบ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่ และผู้ใช้งาน เป็นผู้รับผิดชอบตามภารกิจ ดังนี้

2.1 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เป็นผู้รับผิดชอบ ดังนี้

2.1.1 ควบคุม ติดตาม และตรวจสอบการใช้งานระบบสารสนเทศให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2.1.2 ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

2.1.3 ควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบสารสนเทศ ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

2.1.4 ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

2.1.5 ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

2.1.6 ปฏิบัติงานอื่นๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน

2.2 ผู้ใช้งานเป็นผู้เข้าถึงและใช้งานระบบสารสนเทศตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้อย่างเคร่งครัด