แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ (องค์การมหาชน)

สารบัญ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ (องค์การมหาชน)

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้สำนักงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของ สำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ (องค์การมหาชน) เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยด้านสารสนเทศและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ทั้งภายในและภายนอก

อาศัยอำนาจตามข้อบังคับคณะกรรมการบริหารสำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ เห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ ไว้ดังนี้

๒. วัตถุประสงค์

๒.๑ จัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ที่มีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบยอมรับ และปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๔ เพื่อดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย ๑ ครั้ง ต่อปี

๓. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจ และนโยบายขององค์กร

๓.๒ มุ่งกำหนดแนวทางปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๓.๓ เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๓.๔ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของสำนักงานเองและของสำนักงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการเรียนรู้อย่างต่อเนื่อง

๓.๕ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

๔. องค์ประกอบของนโยบาย

๔.๑ คำนิยาม
๔.๒ แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ
๔.๓ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
๔.๔ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ
๔.๕ แนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน
๔.๖ แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย
๔.๗ แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ
๔.๘ แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
๔.๙ แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ
๔.๑๐ แนวปฏิบัติในการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
๔.๑๑ แนวปฏิบัติในการใช้งานอินเทอร์เน็ต
๔.๑๒ แนวปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์
๔.๑๓ แนวปฏิบัติในการจัดทาระบบสารองข้อมูลและสารสนเทศ
๔.๑๔ แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
๔.๑๕ แนวปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วย วัตถุประสงค์ แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและสำนักงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม ประกอบด้วย

๑. สำนักงาน หมายถึง สำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ (องค์การมหาชน) และสำนักงานสาขา

๒. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงาน

๓. **ผู้บริหารระดับสูงสุด** (Chief Executive Officer: CEO) หมายถึง ผู้บังคับบัญชาสูงสุดของสำนักงาน (ผู้อำนวยการสำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ (องค์การมหาชน)) ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย กำหนดทิศทางรวมทั้งมอบหมายงานให้ผู้ปฏิบัติที่เกี่ยวข้อง กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์ใช้งานไม่ได้ ตลอดจนรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบสารสนเทศไม่ว่ากรณีใดๆ

๔. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) หมายถึง ผู้บังคับบัญชาสูงสุดในด้านเทคโนโลยีสารสนเทศของสำนักงาน (ผู้อำนวยการกลุ่มกิจการ รักษาการแทนรองผู้อำนวยการ(กลุ่มภารกิจด้านยุทธศาสตร์ นวัตกรรม และองค์ความรู้))

๕. กลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ หมายถึง สำนักงานที่ดูแลและบริหารจัดการระบบเทคโนโลยีสารสนเทศ

๖. ผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ หมายถึง หัวหน้าส่วนงานที่ดูแลและบริหารจัดการระบบเทคโนโลยีสารสนเทศของสำนักงาน

๗. การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของสำนักงาน

๘. มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

๙. ขั้นตอนการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

๑๐. แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

๑๑. ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของสำนักงาน โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งสำนักงานกำหนดไว้ดังนี้

ก. ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของสำนักงาน เช่น ผู้อำนวยการ รองผู้อำนวยการ ผู้อำนวยการกลุ่มแผนงาน เป็นต้น

ข. ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

ค. เจ้าหน้าที่ หมายถึง เจ้าหน้าที่และลูกจ้าง พนักงานจ้างประจำกิจกรรม/โครงการต่างๆ ของสำนักงาน

๑๒. สำนักงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่สำนักงานอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของสำนักงาน

๑๓. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

๑๔. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

๑๕. ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๑๖. ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ขององค์กร

๑๗. ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในสำนักงานเข้าด้วยกัน

๑๘. ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของสำนักงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สำนักงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริหาร การพัฒนาและควบคุมการติดต่อสื่อสาร

๑๙. พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace) หมายถึง พื้นที่ที่สำนักงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

- พื้นที่ทำงานทั่วไป (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาเพื่อปฏิบัติงานในสำนักงาน
- พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area)
- พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
- พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)
- พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN coverage area)

๒๐. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๒๑. สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

๒๒. สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

๒๓. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

๒๔. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ ทั้งนี้ รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๒๕.เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๒๖.สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๒๗.จดหมายอิเล็กทรอนิกส์ (Email) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร

ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

๒๘.รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๒๙.ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

กระบวนการตรวจสอบภายใน

๑. วัตถุประสงค์

เพื่อจัดตั้งคณะทำงานรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทำการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง ร่วมกำหนดนโยบาย มาตรฐานหรือบรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง ตลอดจนการกำหนดขั้นตอนการรายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์เพื่อการควบคุมและตรวจสอบภายในสำนักงาน

๒. แนวทางปฏิบัติกระบวนการตรวจสอบภายใน

๒.๑ จัดตั้งคณะทำงานรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีหน้าที่กำหนดแนวนโยบายและแนวปฏิบัติด้านการรักษาความปลอดภัยด้านสารสนเทศของสำนักงาน และทบทวนปรับปรุงการรักษาความปลอดภัยของสารสนเทศของสำนักงาน

๒.๒ กำหนดแผนการตรวจสอบและประเมิน โดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้ทราบถึงระดับความเสี่ยงและความมั่นคงปลอดภัยสารสนเทศของหน่วยงานอย่างน้อย จำนวน ๑ ครั้งต่อปี ทั้งนี้ขึ้นอยู่กับการจัดทำงบประมาณประจำปี

แนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ

๑. บทบาทและความรับผิดชอบ

การกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศ ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศ เกิดความเสียหายหรืออันตรายใดๆ ต่อ สพภ. หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สพภ. และป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่น และการเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต โดยได้กำหนดบทบาทและความรับผิดชอบให้เป็นไปตามหน้าที่ที่ได้รับมอบหมาย ดังนี้

๑. ผู้อำนวยการสำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ(องค์การมหาชน) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพภ.

๒. ผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ มีหน้าที่จัดทำและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สพภ. โดยกำหนดมาตรการและกำกับดูแลการใช้งานและผลักดันให้เจ้าหน้าที่ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สพภ.

๓. ผู้ดูแลระบบ มีหน้าที่ควบคุม ติดตาม และตรวจสอบการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพภ. ให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สพภ.

๔. ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพภ. ตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สพภ.

๒. หน้าที่ความรับผิดชอบของผู้ดูแลระบบ

๑. จัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

๒. บริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์ และระบบเครือข่ายหลักของ สพภ. เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหาย ใช้งานไม่ได้ หรือสูญหาย

๓. เก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพภ. และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

๔. กำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพภ. ตามที่ได้รับมอบหมาย โดยกำหนดสิทธิให้ผู้ใช้งานสามารถใช้งานได้ตามภารกิจของผู้ใช้งาน และสามารถเข้าใช้ได้แต่เพียงงานที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๕. บริหารจัดการการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพภ. ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติให้รีบดาเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สพภ. ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทาดังกล่าวในทันทีและในกรณีจำเป็น เพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นต่อ สพภ. ให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานดังกล่าวทันที

๖. ติดตั้งและเปลี่ยนแปลงค่า parameter ต่างๆ ของระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพภ. ที่ได้รับมอบหมาย และทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยเดือนละครั้ง

๗. บริหารจัดการข้อมูลคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ที่เกี่ยวข้องกับการปฏิบัติงานของ สพภ. สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วง ให้มีความปลอดภัย

๘. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการของ สพภ. เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้งานและต้องเก็บรักษาไว้อย่างครบถ้วนถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และประกาศกระทรวงไอซีทีเรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐

๙. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

๑๐. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๑๑. คืนทรัพย์สินของ สพภ. ที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้บริหารของ สพภ. หรือผู้ที่ได้รับมอบหมาย เพื่อการตรวจสอบการคืนทรัพย์สิน

๓. หน้าที่ความรับผิดชอบของผู้ใช้งาน

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพภ. โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีแนวทางปฏิบัติ ดังนี้

๑. การใช้งานรหัสผ่าน (Password Use) ผู้ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพภ. ควรปฏิบัติตามข้อกำหนดในการใช้งานรหัสผ่าน ดังนี้

(๑) เก็บรหัสผ่านไว้เป็นความลับ

(๒) หลีกเลี่ยงการบันทึกรหัสผ่าน (เช่น บันทึกลงในกระดาษ ในแฟ้มข้อมูล หรือในอุปกรณ์พกพาต่าง ๆ) นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัยและวิธีการในการบันทึกได้รับการอนุมัติแล้ว

(๓) เปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหลได้

(๔) กำหนดรหัสผ่านที่มีคุณภาพและมีความยาวเพียงพอสำหรับ

(๔.๑) ง่ายสำหรับจดจำ

(๔.๒) ไม่อยู่บนพื้นฐานของสิ่งที่คนอื่นสามารถคาดเดาได้ง่ายหรือสามารถหาได้จากข้อมูลเกี่ยวกับตน เช่น ชื่อ หมายเลขโทรศัพท์และวันเกิด เป็นต้น

(๔.๓) ไม่สร้างจุดอ่อนโดยการใช้คำที่อยู่ในพจนานุกรม

(๔.๔) ไม่มีคำซ้ำหรือตัวอักษรซ้ำ ไม่ควรเป็นตัวเลขทั้งหมด หรือไม่ควรเป็นตัวอักษรทั้งหมด

(๕) เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้ที่ได้สิทธิ์พิเศษควรได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ) และหลีกเลี่ยงการวนใช้รหัสผ่านเดิมที่เคยใช้แล้ว

(๖) กำหนดให้เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

(๗) ไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ Login อัตโนมัติ

(๘) ไม่ใช้รหัสผ่านร่วมกับผู้อื่น

(๙) ไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ในการปฏิบัติงานและในกรณีใช้ส่วนตัว

(๑๐) ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัว ควรแนะนำให้ใช้รหัสผ่านเดียวกันที่มีคุณภาพข้างต้นสำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านั้นควรมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

คุณสมบัติของรหัสผ่านที่ดี

(๑) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

(๒) ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผนและง่ายต่อการคาดเดา เช่น “abcdef” “aaaaaa” “๑๒๓๔๕” “12345”

(๓) ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

(๔) ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

(๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน ๓ ครั้ง

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายคอมพิวเตอร์

(๗) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

(๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

(๑) ผู้ใช้งานควรออกจากระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพภ. โดยทันทีเมื่อเสร็จสิ้นงานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน เช่น ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องโน๊ตบุ๊ก

(๒) ผู้ใช้งานควรล็อค (Lock) อุปกรณ์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

(๓) ผู้ใช้งานควรป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศและการสื่อสารของตน โดยต้องใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

(๔) ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่าน ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของสำนักงานร่วมกัน

(๕) ผู้ใช้งานและผู้ดูแลระบบต้องตั้งให้เครื่องคอมพิวเตอร์ล็อค (Lock) หน้าจอ หลังจากที่ไม่ได้ใช้งาน มาช่วงระยะเวลาหนึ่ง เช่น ๑๐ นาที หลังจากที่มีการล็อค (Lock) หน้าจอแล้วนั้น ต้องใส่รหัสผ่านให้ถูกต้อง จึงจะสามารถเปิดหน้าจอเพื่อเข้าถึงเครื่องคอมพิวเตอร์หรือระบบงานได้

(๖) ปิดเครื่องคอมพิวเตอร์ (Personal Computer) ที่ตนเองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้นหรือไม่มีการใช้งานนานเกินกว่า ๑ ชั่วโมง เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องแม่ข่ายที่ให้บริการซึ่งต้องใช้งานตลอด ๒๔ ชั่วโมง

(๗) ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้เจ้าหน้าที่เข้าใจในมาตรการป้องกันที่ได้กำหนดไว้นั้น

๓. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์

การควบคุมทรัพย์สินสารสนเทศ (clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูลและแฟ้มข้อมูล เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ระบบสารสนเทศและข้อมูลสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ มีแนวทางปฏิบัติ ดังนี้

(๑) ผู้ใช้งานต้องป้องกันทรัพย์สินของ สพภ. และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศ ที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย โดยให้ครอบคลุมเรื่องต่างๆ ประกอบด้วย

- การจัดการบริเวณล้อมรอบ
- การควบคุมการเข้า - ออกพื้นที่
- การจัดบริเวณการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก
- การวางอุปกรณ์
- ระบบและอุปกรณ์สนับสนุนการทำงาน

(๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ
- วัฒนธรรมองค์กร

(๓) ต้องมีการป้องกันเครื่องคอมพิวเตอร์หรือระบบงานของ สพภ. ก่อนเข้าใช้งาน โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสม

(๔) ต้องมีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของ สพภ.
- จัดเก็บเอกสาร ข้อมูลในการทำงาน ข้อมูลสำคัญหรือลับ หรือสื่อบันทึกข้อมูล ไว้ในสถานที่ที่มีความปลอดภัยภายหลังจากใช้งานเสร็จ เช่น เก็บไว้ในตู้ที่ล็อคกุญแจได้ เป็นต้น
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันเครื่องโทรสารที่ใช้ในการติดต่อสื่อสารหรือส่งข้อมูลสำคัญ เมื่อไม่มีผู้ใช้งาน
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารสำคัญหรือลับออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ
- ในกรณีที่ต้องการนำทรัพย์สินสารสนเทศต่างๆ เช่น เอกสาร สื่อบันทึกคอมพิวเตอร์ หรือสารสนเทศ ออกจาก สพภ. ต้องขออนุมัติจากผู้บังคับบัญชาก่อนทุกครั้ง

(๕) ผู้ดูแลระบบต้องจัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

(๖) ผู้ดูแลระบบต้องบริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์และระบบเครือข่ายหลักของ สพภ. เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหายใช้งานไม่ได้ หรือสูญหาย

(๗) ผู้ดูแลระบบต้องเก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

(๘) ในการทำลายข้อมูลลับ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้วิธีการหัก ,บดให้เสียหาย หรือเผาทำลาย
เทป	จะต้องทำการลบข้อมูลทั้งม้วนเทป (Erase) ผ่าน Tape Device ก่อนการทำลาย โดยใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แม็ต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

๔. การเข้าถึงและควบคุมการใช้งานระบบคอมพิวเตอร์หรือสารสนเทศ

ต้องจัดทำนโยบายและแนวปฏิบัติในการควบคุมการเข้าถึงอย่างเป็นลายลักษณ์อักษร และปรับปรุงอย่างน้อยปีละ ๑ ครั้ง โดยการจัดทำนโยบายนี้จะพิจารณาจากความต้องการทางการปฏิบัติงาน และทางด้านความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ ซึ่งมีแนวทางปฏิบัติ ดังนี้

(๑) การควบคุมการเข้าถึงเครือข่าย (Network access control)

- ต้องจัดทำนโยบายการใช้งานบริการเครือข่าย (Policy on use of network services) ซึ่งจะต้องครอบคลุมถึงการระบุว่าบริการใดที่อนุญาตให้ผู้ใช้งานสามารถใช้งานได้ บริการใดไม่สามารถใช้งานได้
- ต้องมีการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกสำนักงาน (User authentication for external connections) ก่อนที่จะอนุญาตให้เข้าใช้งานเครือข่ายและระบบสารสนเทศของสำนักงาน ได้
- ต้องมีการพิสูจน์ตัวตนอุปกรณ์บนเครือข่าย (Equipment identification in networks) ให้สามารถระบุและพิสูจน์ตัวตน เพื่อบ่งบอกว่าการเชื่อมต่อนั้นมาจากอุปกรณ์หรือสถานที่ที่ได้รับอนุญาตแล้ว
- ต้องมีการแบ่งแยกเครือข่าย (Segregation in networks) ตามกลุ่มของบริการสารสนเทศที่ใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ
- ต้องมีการควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) โดยต้องจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่ายระหว่างองค์กร การเชื่อมต่อต้องเป็นไปตามนโยบายในการควบคุมการเข้าถึงและข้อกำหนดที่แอพพลิเคชั่นที่ใช้งานทางการปฏิบัติงานได้ระบุไว้
- ต้องมีการควบคุมการกำหนดเส้นทางบนเครือข่าย (Network routing control) เพื่อควบคุมการเชื่อมต่อทางเครือข่ายและการไหลเวียนของสารสนเทศบนเครือข่ายให้เป็นไปตามนโยบายในการควบคุมการเข้าถึง

(๒) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

- ผู้ใช้บริการต้องกำหนดชื่อผู้ใช้ และรหัสผ่าน ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน

- ผู้ใช้บริการไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่าน ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของสำนักงานร่วมกัน

- ผู้ใช้บริการต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งานภายใน ๑๐ นาทีหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน เพื่อเข้าใช้งาน

- ผู้ใช้บริการต้องทำ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

- ควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยง

(๓) การควบคุมการเข้าถึงแอพพลิเคชั่นและสารสนเทศ (Application and information access control)

- ต้องมีการจำกัดการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของแอพพลิเคชั่น (Information access restriction) โดยการเข้าถึงจะต้องแยกตามประเภทของผู้ใช้งาน

- ต้องมีการแยกระบบสารสนเทศที่มีความสำคัญสูง (Sensitive system isolation) ไว้ในบริเวณที่แยกต่างหากออกมา สำหรับระบบนี้โดยเฉพาะ

(๔) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ มีแนวปฏิบัติ ดังนี้

- ทำการประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสม สำหรับข้อมูลที่จำเป็นต้องป้องกัน

- กำหนดหลักการทั่วไปสำหรับการป้องกันข้อมูลโดยใช้การเข้ารหัสข้อมูล

- การจัดเก็บ username และ password ของระบบสารสนเทศลงในฐานข้อมูลใดๆ จะต้องทำการเข้ารหัสด้วย MD5 ใน field ของ password ก่อนบันทึกลงในฐานข้อมูลทุกครั้ง

- ต้องมีการเชื่อมต่อโดยการเข้ารหัส SSL ผ่านโปรโตคอล https สำหรับระบบสารสนเทศแบบ web application ที่มีชั้นหรือระดับความลับ/สำคัญมาก เพื่อเป็นการเข้ารหัสข้อมูลที่ส่งระหว่างบราว์เซอร์และเว็บเซิร์ฟเวอร์

- กำหนดช่องทางการรับ – ส่งข้อมูลสำคัญหรือข้อมูลลับที่เหมาะสมกับสำนักงาน สำหรับช่องทางดังต่อไปนี้

  - ระบบการสื่อสารข้อมูล ซึ่งรวมถึง LAN และอินเทอร์เน็ต
  - เครือข่ายไร้สายและอุปกรณ์เครือข่ายไร้สาย
  - สื่อบันทึกข้อมูลที่สามารถถอดแยกได้ (จากตัวเครื่องคอมพิวเตอร์)

- กำหนดวิธีการในการบริหารจัดการและการใช้งานกุญแจสาหรับการเข้ารหัสข้อมูลดังนี้

  - วิธีการป้องกันกุญแจที่ใช้สาหรับการเข้ารหัสข้อมูล
  - วิธีการกู้คืนข้อมูลที่ถูกเข้ารหัสไว้ในกรณีที่กุญแจเกิดการสูญหายหรือถูกทำให้เสียหาย

  - บทบาทและผู้มีหน้าที่รับผิดชอบที่เกี่ยวข้องกับการเข้ารหัสข้อมูล ประกอบด้วย ผู้ทำหน้าที่ควบคุมและดูแลกุญแจ การสร้างกุญแจ ผู้ทำหน้าที่ทำลาย ผู้ใช้งาน ผู้ทำหน้าที่จัดการกรณีกุญแจเกิดการสูญหาย

- ระบุข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลที่เป็นความลับ หรือวิธีการรักษาความลับของข้อมูล ดังนี้

ก) ต้องแสดงชั้นความลับบนไฟล์ข้อมูลลับ และแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

ข) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ด้วยการใช้การเข้ารหัสข้อมูลตามมาตรฐานที่สำนักงานกำหนด

ค) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการกำหนดรหัสผ่านสำหรับไฟล์ที่มีการใช้งาน

- ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายของสำนักงานเพื่ออนุญาตให้ผู้อื่นเข้าถึงได้
- ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอ ในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูล ว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่
- ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่
- ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environment Security)

๑. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย มีแนวทางปฏิบัติ ดังนี้

๑. ให้กลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๒. ให้กลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๓. ให้กลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและห้องจัดเก็บเครื่องแม่ข่ายและอุปกรณ์

๔. สำนักงานภายนอกหรือบุคคลภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในสำนักงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๒. ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

๑. ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผู้ติดต่อ ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ใน สพภ.

๒. ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน เข้ามาปฏิบัติงานในห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ ต้องลงบันทึกรายการอุปกรณ์ ตามที่ระบุไว้ในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ ให้ถูกต้องชัดเจน

๓. ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อ กับผู้ดูแลระบบ ซึ่งผู้ดูแลระบบต้องตรวจสอบการคืนบัตรและตรวจสอบการลงบันทึกตามเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ ทุกครั้ง

๔. ผู้ดูแลระบบ ควรตรวจสอบความถูกต้องของข้อมูลที่บันทึกในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ เป็นประจำทุกเดือน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านสารสนเทศ

๑. การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy)

ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของสำนักงาน มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๑.การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

๒.ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในสำนักงาน ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB client หรือ Wireless card

๓.ห้ามผู้ใช้งาน (User) เปิด ad-hoc หรือ peer-to-peer Network

๔.กรณีที่ผู้บังคับบัญชาอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

๔.๑ ผู้ดูแลระบบต้องวาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดยจะต้องวาง Access Point หน้า Firewall และหากมีความจำเป็นจริงๆ ต้องวางในระบบเครือข่ายภายใน ที่เป็น Internal Network ต้องเพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption)

๔.๒ ให้ผู้ใช้กรอกรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น ให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๔.๓ ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตทันทีที่นำ Access Point มาใช้งาน และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัว Access Point ด้วย

๔.๔ ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

๔.๕ ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

๔.๖ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือสำนักงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของสำนักงาน

๔.๗ ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศทราบทันที

๒.การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy)

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์(Firewall) ของสำนักงานมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๑. กลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ มีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของไฟร์วอลล์ทั้งหมดของสำนักงาน

๒. การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

๓. ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

๔. ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการ Authentication ทุกครั้งก่อนการใช้งานด้วย รหัสผู้ใช้ (User account) และรหัสผ่าน (User password)

๕. ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

๖. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ดูแลระบบที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๗. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๘. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่ทางสำนักงานอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับอนุญาตจากผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ ก่อน

๙. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อนโยบายจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง และการกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ในเครือข่าย ต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ โดยต้องระบุข้อมูลดังนี้

๙.๑ หมายเลข Port ที่ต้องการขอให้เปิด

๙.๒ หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

๙.๓ วัตถุประสงค์ หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้นๆ

๙.๔ วันที่เริ่มใช้ และวันที่สิ้นสุดการขอใช้

๑๐. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

๑๑. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

๑๒. สำนักงานมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบของสำนักงาน หรือกฎหมาย หรืออาจทำให้เกิดการทำงานของโปรแกรม ที่มีความเสี่ยงต่อความปลอดภัยของระบบเทคโนโลยีสารสนเทศ จนกว่าจะได้รับการแก้ไข

๑๓. ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศระเบียบ ของสำนักงาน หรือกฎหมาย หรืออาจจะทำให้เกิดความเสี่ยงด้านความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของสำนักงาน กลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศจะยกเลิกการให้บริการทันที

๑๔. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาก่อน

๓. การรักษาความมั่นคงปลอดภัยของระบบตรวจจับการบุกรุก (Intrusion Detection System/Intrusion Prevention System Policy : IDS/IPS Policy)

IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบเทคโนโลยีสารสนเทศ และข้อมูลบนเครือข่ายภายในสำนักงาน ให้มีความมั่นคงปลอดภัย แนวทางการปฏิบัติและบทบาทหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับการตรวจสอบการบุกรุกเครือข่าย เป็นดังนี้

๑. IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของสำนักงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

๒. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๓. ระบบทั้งหมดใน DMZ จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

๔. โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

๕. มีการตรวจสอบและ Update Patch/Signature ของ IDS/IPS เป็นประจำ

๖. มีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

๗. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ ที่ใช้ในการเข้าถึงเครือข่ายของระบบเทคโนโลยีสารสนเทศตามปกติ

๘. เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

๙. พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

๑๐. พฤติกรรม กิจกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ ที่ถูกค้นพบ จะต้องมีการรายงานให้ผู้บังคับบัญชาทราบ ภายใน ๑ ชั่วโมงที่ตรวจพบ

๑๑. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

๑๒. มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ ป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และดำเนินการตามแผน

๑๓. สำนักงานมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๑๔. การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น และผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของสำนักงาน การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบเทคโนโลยีสารสนเทศ จะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของสำนักงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

๔.การป้องกันไวรัสและภัยคุกคามอื่นๆ ในการใช้งานคอมพิวเตอร์

๑. ผู้ใช้งานควรทำการสำรองข้อมูลสำคัญที่อยู่บนเครื่องคอมพิวเตอร์ไว้ เช่น บนแผ่น CD หรือ DVD หรือ Flash Drive หรือ Memory Card เพื่อลดปัญหาการกู้คืนข้อมูลที่ถูกทำลายโดยไวรัสคอมพิวเตอร์

๒. ห้ามผู้ใช้งานปรับแต่ง หรือยกเลิกการทำงานของซอฟต์แวร์ป้องกันไวรัส ที่สำนักงานติดตั้งให้

๓. ผู้ใช้งานควรมีส่วนร่วมในการบำรุงรักษาซอฟต์แวร์ป้องกันไวรัสที่ใช้ โดยตรวจสอบว่ามีการ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอยู่เสมอ และแจ้งให้ทราบหากไม่สามารถ Update ซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยได้

๔. ผู้ใช้งานต้องแจ้งให้ทราบ เมื่อพบว่าคอมพิวเตอร์หรือซอฟต์แวร์ที่ใช้มีพฤติกรรมผิดไปจากปกติ หรือเมื่อสงสัยว่ามีการติดไวรัส

๕. ผู้ใช้งานต้องตรวจสอบข้อมูลหรือโปรแกรมที่ได้รับจากผู้อื่นทุกครั้ง เมื่อมีการติดตั้งหรือใช้งาน ด้วยซอฟต์แวร์ป้องกันไวรัส และหากตรวจพบไวรัสจะต้องรีบจัดการทำลายไวรัสโดยเร็วที่สุด หากไม่สามารถกำจัดไวรัสที่ติดมากับข้อมูลหรือโปรแกรมนั้น ห้ามทำการเปิดข้อมูลหรือติดตั้งโปรแกรมลงไปบนเครื่องที่ใช้งานอยู่เด็ดขาด

แนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน

แนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) มีวิธีการปฏิบัติ ดังนี้

๑.การลงทะเบียนผู้ใช้งาน (User Registration)

๑. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศขององค์กร

๒. ผู้ดูแลระบบต้องตรวจสอบว่าผู้ใช้ได้รับมอบหมายสิทธิ์จากเจ้าของระบบสำหรับการใช้งานระบบสารสนเทศและบริการอย่างถูกต้อง ต้องมีการอนุมัติรับรองการได้สิทธิ์จากผู้บริหารอย่างชัดเจน

๓. ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๔. ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และมีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยขององค์กร

๕. ผู้ดูแลระบบต้องมอบเอกสารรับรองสิทธิ์การเข้าถึงแก่ผู้ใช้ เพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๖. ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยี สารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๗. การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๘. การลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๘.๑ เจ้าหน้าที่ใหม่ขององค์กรกรอกข้อมูลคำขอใช้บริการลงแบบ ฟอร์มลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ เช่น คำขอใช้อินเตอร์เน็ต ระบบอีเมล์ หรือระบบงานต่าง ๆ

๘.๒ ยื่นคำขอกับผู้อำนวยการศูนย์สารสนเทศ หรือเจ้าหน้าที่ศูนย์สารสนเทศผู้ที่ได้รับมอบหมาย

๒.การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

๑. การให้สิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

๑.๑ ผู้ดูแลระบบตรวจสอบข้อมูลในแบบฟอร์ม ซึ่งข้อมูลจะต้องครบถ้วนทั้งหมด พร้อมทั้งต้องมีลายเซ็นของผู้ขอเข้าใช้งานระบบ ลายเซ็นของบุคคลผู้มีสิทธิ์อนุญาตในการลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๑.๒ ผู้ดูแลระบบตรวจสอบความซ้ำซ้อนของบัญชีผู้ใช้งาน

๑.๓ ผู้ดูแลระบบให้สิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม

๒. การแจ้งยกเลิกสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๑ หัวหน้างานหรือผู้บังคับบัญชา กรอกข้อมูลลงในแบบฟอร์ม และยื่นคำขอกับผู้อำนวยการศูนย์สารสนเทศ

๒.๒ ผู้ดูแลระบบยกเลิกสิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม และลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด

๓.ระบบบริหารจัดการรหัสผ่าน (Password management system)

๑. ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคลเพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

๒. ระบบบริหารจัดการรหัสผ่าน ต้องอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง และมีขั้นตอนปฏิบัติ เพื่อยืนยันรหัสผ่านใหม่ที่ตั้ง

๓. ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้ผู้ใช้งานเลือกรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น เช่น ไม่ใช้ชื่อ นามสกุล วันเกิด หมายเลขโทรศัพท์ คำจากพจนานุกรม เป็นต้น

๔. ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุกๆ ๖ เดือน

๕. ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีที่ได้รับบัญชีผู้ใช้งานและทำการล็อกอินเข้าใช้งานระบบงานเป็นครั้งแรก

๖. ระบบบริหารจัดการรหัสผ่าน ต้องสามารถระบุข้อผิดพลาดในการตั้งรหัสผ่านของผู้ใช้งานได้ เช่น รหัสผ่านมีความยาวของตัวอักขระน้อยกว่าที่กำหนด มีชื่อผู้ใช้งานอยู่ในรหัสผ่าน เป็นต้น

๗. ระบบบริหารจัดการรหัสผ่าน ต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน เช่น ให้แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอ เป็นต้น

๘. ระบบบริหารจัดการรหัสผ่าน ควรป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้ และ/หรือ ที่จาเป็นต้องมีการส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น โดยการเข้ารหัสข้อมูลการคำนวณผลรวม (Hash) เพื่อซ่อนข้อมูลไว้

๔.การบริหารจัดการชื่อผู้ใช้งานและรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๑. ผู้ดูแลระบบต้องกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งาน หรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ

๒. ผู้ดูแลระบบมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยพิจารณาจากลำดับชั้นความลับของข้อมูล หรือความสำคัญตามภารกิจ และรหัสผ่านที่กำหนดใหม่ ต้องไม่ซ้ำกับรหัสผ่านเดิม

๓. ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านที่ได้รับ โดยทันที

๔. ผู้ใช้งานต้องกำหนดรหัสผ่านและเปลี่ยนรหัสผ่านของตนเองในการใช้งานตามหลักเกณฑ์ ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใด ๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๕. ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับ และระมัดระวังปูองกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่น และไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใด ๆ ทั้งสิ้น เว้นแต่ กรณีผู้ใช้งานที่มีอำนาจอนุมัติใด ๆ ในระบบเทคโนโลยีสารสนเทศไม่สามารถปฏิบัติราชการอันจะเป็นเหตุให้ระบบเทคโนโลยีสารสนเทศไม่สามารถดำเนินการต่อไปได้ ให้แต่งตั้งผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าวเพื่อใช้เป็นหลักฐานในการตรวจสอบการใช้สิทธิ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้วให้ผู้ใช้งานซึ่งเป็นเจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที

๖. กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

๗. ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผนและง่ายต่อการคาดเดา เช่น “abcdef” “aaaaaa” “๑๒๓๔๕” “12345”

๘. ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

๙. ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

๑๐. กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน ๓ ครั้ง

๑๑. ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายคอมพิวเตอร์

๑๒. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

๑๓. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๑๔. ในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ ให้ผู้ใช้งานออกจากระบบ (Log off) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบเทคโนโลยีสารสนเทศต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหลต้องเปลี่ยนรหัสผ่านทันที

๑๕. เมื่อมีปัญหาการใช้งานชื่อผู้ใช้งานและรหัสผ่าน ให้ติดต่อผู้ดูแลระบบ เช่น ลืมชื่อผู้ใช้งานหรือรหัสผ่าน

๑๖. การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย โดยใส่ซองปิดผนึก และประทับตรา “ลับ” และส่งไปยังผู้ใช้งาน และแนบเอกสาร “แนวปฏิบัติสำหรับการบริหารจัดการชื่อผู้ใช้งานและรหัสผ่าน” รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามระเบียบดังกล่าวโดยเคร่งครัด

๕.การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

๑. ผู้ดูแลระบบดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง

๒. ผู้ดูแลระบบทบทวนสิทธิ์สำหรับผู้ที่มีสิทธิในระดับสูง เช่น สิทธิในระดับผู้ดูแลระบบ ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๓. ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใดๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

๔. ผู้ดูแลระบบต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

๕. ผู้ดูแลระบบต้องดำเนินการตรวจสอบสิทธิและติดตามการใช้งานตามสิทธิที่ได้รับของแต่ละระบบ

๖. ผู้ดูแลระบบต้องกำหนดให้มีการเพิกถอนสิทธิหรือระงับการใช้งานของแต่ละสิทธิแตกต่างกันไปตามหน้าที่ที่รับผิดชอบในแต่ละระบบ

แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย

แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต มีดังต่อไปนี้

๑.การใช้งานบริการระบบเครือข่าย มีแนวทางปฏิบัติ ดังนี้

๑. ห้ามผู้ใช้งานกระทำการใดๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานต้องรับรองว่า หากมีการกระทำการใดๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของ สพภ.

๒. สพภ. ไม่อนุญาตให้ผู้ใช้งานกระทำการใดๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความ การซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๓. ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว สพภ. ไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๔. ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

๕. สพภ. ให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

๖. บัญชีผู้ใช้งาน (User Account) ที่ สพภ. ให้กับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่างๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่างๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้นๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๗. ผู้ใช้บริการระบบเครือข่าย สพภ. ต้องพิสูจน์ยืนยันตัวตน (Authentication) ทุกครั้งที่ใช้บริการ

๘. การใช้งานบริการระบบเครือข่าย สพภ. กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๙. ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

๒.ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

๑. ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการลงบันทึกข้อมูลในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ สพภ.

๒. เจ้าหน้าที่ต้องตรวจสอบความถูกต้องของข้อมูลที่บันทึกในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ สพภ. เป็นประจำทุกเดือน

๓. ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

๔. ในกรณีที่ผู้ใช้งานต้องการเข้าถึงเครือข่ายจากภายนอก สพภ. โดยต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของสำนักงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ การเข้าสู่ระบบเครือข่ายจะต้องเชื่อมผ่านด้วย วิธีการ Remote Access VPN หรือ FTP โดยผู้ใช้งานจะต้องพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการป้อนชื่อผู้ใช้งาน(User name) และรหัสผ่าน (Password) เพื่อยืนยันตัวตนของผู้ใช้งาน ในการเข้าถึงเครือข่ายในส่วนที่ได้รับอนุญาต

๕. มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะ ต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้รหัสผ่าน (Password) เป็นต้น

๖. ตรวจสอบผู้ใช้งานเมื่อมีการเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต

๓.การระบุอุปกรณ์บนเครือข่าย มีแนวทางปฏิบัติ ดังนี้

๑. ทำการระบุหมายเลขอุปกรณ์บนเครือข่าย ประกอบด้วย หมายเลขเทอร์มินัล หมายเลข MAC Addressและหมายเลข IP Address

๒. ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

๓. มีการใช้ไฟร์วอลล์หรืออุปกรณ์เครือข่ายอื่นๆ เพื่อกำหนดว่าหมายเลขระบุอุปกรณ์ใดจะสามารถเข้าถึงเครือข่ายส่วนใดของ สพภ.

๔. มีการรักษาความมั่นคงปลอดภัยทางกายภาพต่ออุปกรณ์คอมพิวเตอร์หรือเครือข่าย เพื่อป้องกันการเปลี่ยนแปลงแก้ไขหมายเลขระบุอุปกรณ์เหล่านั้น

๕. อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

๖. กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่

๗. จัดทำแผนผังระบบเครือข่าย ประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก โดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

๘. ทำการทบทวนแผนผังเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

๔.การป้องกันพอร์ตที่ใช้สาหรับตรวจสอบและปรับแต่งระบบ มีแนวทางปฏิบัติ ดังนี้

๑. ทำการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบ ทั้งทางกายภาพและโดยการล็อกอินเข้ามาใช้งาน

๒. ทำการล็อคอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่าคอนฟิกกูเรชันด้วยกุญแจ เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์และทาการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

๓. ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๔. ผู้ดูแลระบบต้องกำหนดการเปิด - ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่างๆ โดยจะปิดพอร์ตที่เสี่ยงและก่อให้เกิดความเสียหายต่อระบบเครือข่าย

๕. ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมอ เช่น อย่างน้อยเดือนละ ๑ ครั้ง

๖. มีการกำหนดสิทธิบุคคล ในการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์สำนักงาน โดยให้เฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องเท่านั้น

๗. ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์สำนักงาน หากมีความจำเป็นต้องเข้า จะต้องให้เจ้าหน้าที่ เป็นผู้รับผิดชอบนำพาเข้าไป

๘. บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใดๆ ในห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์สำนักงาน จะต้องลงชื่อในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการฯ ให้ถูกต้อง และได้รับการอนุมัติจากผู้อำนวยการกลุ่มการกิจการองค์ความรู้และเทคโนโลยีสารสนเทศก่อน ซึ่งต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

๙. บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่าย หรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้อำนวยการกิจการองค์ความรู้และเทคโนโลยีสารสนเทศก่อน

๑๐. มีการติดตั้งระบบป้องกันและตรวจสอบการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์สำนักงานอย่างปลอดภัย เช่น การใช้ระบบชีวภาพ (Biometric) หรือ สมาร์ทการ์ด (Smartcard) และติดตั้งกล้องโทรทัศน์วงจรปิดป้องกันการโจรกรรม เป็นต้น

๕.การแบ่งแยกเครือข่าย มีแนวทางปฏิบัติ ดังนี้

๑. ทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการ ผู้ใช้งาน และระบบงานต่างๆ ของ สพภ.

๒. มีการใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่าย ทั้งจากภายในและภายนอก ซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของ สพภ.

๓. มีการแยกกลุ่มเครือข่ายเป็น ๔ ประเภทใหญ่ๆ คือ

๑) ระบบเครือข่ายภายใน

๒) ระบบเครือข่ายภายนอก

๓) ส่วนที่มีความสำคัญสูงใน DMZ Zone (Demilitarized Zone) ที่เชื่อมต่อทั้งเครือข่ายภายในและเครือข่ายภายนอก

๔) เครือข่ายสำหรับติดตั้งระบบงานสารสนเทศต่างๆ ของ สพภ.

๔. มีการจัดทำผังเครือข่ายที่แสดงถึงขอบเขตที่ครอบคลุมแต่ละส่วนที่แบ่งแยก โดยมีการปรับปรุงให้เป็นปัจจุบันหรืออย่างน้อยปีละครั้ง

๖.การควบคุมการเชื่อมต่อทางเครือข่าย มีแนวทางปฏิบัติ ดังนี้

๑. มีการตรวจสอบ และจำกัดผู้ใช้งานในการเชื่อมต่อทางเครือข่าย ที่สอดคล้องกับนโยบายควบคุมการเข้าถึงและข้อกำหนดของระบบงานที่ได้ระบุไว้

๒. มีการจำกัดสิทธิและความสามารถของผู้ใช้งาน ในการเชื่อมต่อเข้าสู่ระบบเครือข่ายของสำนักงาน

๓. มีการระบุอุปกรณ์และเครื่องมือที่ใช้ในการควบคุมการเชื่อมต่อระบบเครือข่ายของสำนักงาน

๔. มีการควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายของสำนักงานโดยไม่ได้รับอนุญาต

๕. มีการใช้ไฟร์วอลล์ ทำการกรองข้อมูลที่ไหลเวียนในเครือข่าย ให้เป็นไปตามหรือสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายที่ได้กำหนดไว้

๖. มีการจำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งานต่อระบบงานต่างๆ ของสำนักงาน อาทิ ระบบงานที่ใช้ในการส่งข้อความ (Messaging applications) เช่น ระบบอีเมล ระบบงานสาหรับการโอนย้ายไฟล์ ระบบงานต่างๆ สาหรับใช้งานภายในสำนักงาน

๗. มีการจำกัดการเชื่อมต่อทางเครือข่ายของผู้ใช้งาน ตามวันที่ เวลา หรือช่วงเวลาที่อนุญาตให้ใช้งาน

๘. การเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกสำนักงาน จะต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกซึ่งมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี (Malware)

๙. ทำการติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้ระบบเครือข่ายของสำนักงาน ในลักษณะที่ผิดปกติ

๑๐. ห้ามเปิดช่องทางการเชื่อมต่อทางเครือข่ายจากภายนอกเข้าสู่เครือข่ายภายในสำนักงาน เพื่อให้สามารถเข้าถึงเครื่องแม่ข่ายสาหรับระบบงานได้จากระยะไกล ยกเว้นในกรณีที่มีความจำเป็น หรือมีความเร่งด่วนสูง ซึ่งจะต้องได้รับอนุมัติจากผู้บังคับบัญชาก่อนดำเนินการ

๑๑. กำหนดระยะเวลาที่แน่นอนของการเชื่อมต่อจากระยะไกล เช่น ให้ใช้ในระยะเวลา ๗ วัน และหลังจากที่สิ้นสุดการใช้งาน ให้ทำการปิดช่องทางการเชื่อมต่อนั้นโดยทันที

๗.การควบคุมการจัดเส้นทางบนเครือข่าย มีแนวทางปฏิบัติ ดังนี้

๑. ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๒. กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๓. กำหนดมาตรการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้หรือจำกัดสิทธิในการใช้บริการเครือข่าย

แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต มีดังต่อไปนี้

๑.ขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานระบบปฏิบัติการที่มีความมั่นคงปลอดภัย ซึ่งเริ่มตั้งแต่การลงทะเบียน การกำหนดสิทธิ การบริหารจัดการรหัสผ่าน และการทบทวนสิทธิต่างๆ รวมถึงข้อกำหนดเกี่ยวกับการอนุญาตให้เข้าใช้ และกำหนดรายละเอียดอื่นๆ เพิ่มเติม โดยมีแนวทางปฏิบัติ ดังนี้

๑. ผู้ใช้งานระบบปฏิบัติการต้องได้รับการอนุมัติจากผู้บังคับบัญชาอย่างเป็นลายลักษณ์อักษร

๒. ผู้ใช้งานต้องกาหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๓. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน ในระยะเวลา ๑๐ นาที หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๔. ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User name และ Password ทุกครั้ง

๕. มีการจำกัดระยะเวลาในการป้อนรหัสผ่าน และหากผู้ใช้งานป้อนรหัสผ่านผิดเกิน ๓ ครั้ง ระบบจะทำการล็อคสิทธิการเข้าถึงของผู้ใช้งาน ทำให้ผู้ใช้งานรายนั้นไม่สามารถเข้าถึงระบบปฏิบัติการได้อีก จนกว่าผู้ดูแลระบบจะดำเนินการปลดล็อคให้

๖. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

๗. ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๘. ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

๙. ซอฟต์แวร์ที่มีลิขสิทธิของสำนักงาน ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

๑๐. ซอฟต์แวร์ที่สำนักงานจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๑๑. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของสำนักงาน เพื่อประโยชน์ทางการค้า

๑๒. ในกรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม

๑๓. ห้ามผู้ใช้งานใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน ในการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

๒.การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอน ทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวทางปฏิบัติ ดังนี้

๑. มีการตั้งชื่อบัญชีผู้ใช้งานในระบบงานที่แตกต่างกัน เช่น บัญชีของผู้ใช้งานทั่วไป บัญชีของผู้ดูแลระบบบัญชีของผู้ดูแลฐานข้อมูล บัญชีของผู้พัฒนาระบบบัญชีของเจ้าหน้าที่ทางเทคนิคอื่นๆ เป็นต้น

๒. ผู้ใช้งานทุกคนต้องมีชื่อผู้ใช้งานแยกจากกันของแต่ละบุคคล เพื่อใช้ในการพิสูจน์ตัวตนที่แตกต่างกัน

๓. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้ง ก่อนใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน โดยใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๔. ผู้ใช้งานที่สามารถเข้าถึงระบบปฏิบัติการได้ จะต้องได้รับการอนุมัติสิทธิการเข้าถึงระบบปฏิบัติการจากผู้บังคับบัญชาของหน่วยงานหรือเจ้าของระบบงานเท่านั้น

๕. ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้ (Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น เกิดจากการกระทำของผู้อื่น

๖. ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้ (Account) ไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น

๗. ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๓.การใช้งานโปรแกรมอรรถประโยชน์หรือโปรแกรมประเภทยูทิลิตี้ (Use of system utilities)

ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว โดยมีแนวทางปฏิบัติ ดังนี้

๑. ไม่อนุญาตให้ผู้ใช้งานติดตั้งโปรแกรมอื่นๆ ได้เอง ต้องขออนุญาตจากผู้ดูแลระบบและทำหนังสือขอติดตั้ง โดยมีผู้บังคับบัญชาที่เกี่ยวข้องลงนามอนุมัติ หากผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟตแวรอื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือวาเปนความผิดสวนบุคคล ผูใช้งานจะต้องรับผิดชอบแตเพียงผูเดียว

๒. ซอฟตแวร (Software) ที่สำนักงานไดจัดเตรียมไวใหผูใชงาน ถือเปนสิ่งจำเปนตอการทำงานหามมิใหผูใชงานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แกไข หรือทำสำเนาเพื่อนำไปใชงานที่อื่น

๔.การหมดเวลาใช้งานระบบสารสนเทศ (limitation of connection time)

ผู้ดูแลระบบต้องกำหนดให้ระบบสารสนเทศยุติตัวเองลง เมื่อไม่มีการใช้งานในช่วงเวลาหนึ่ง โดยมีแนวทางปฏิบัติ ดังนี้

๑. ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เช่น ระบบงาน และอุปกรณ์เครือข่าย มีการตัดและหมดเวลาการใช้งาน รวมถึงการปิดการใช้งานหลังจากที่ไม่มีกิจกรรมการใช้งานในช่วงระยะเวลา ๑๐ นาที

๒. กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน สำหรับระบบที่มีความเสี่ยงสูงจะต้องมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้น เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓. กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน สำหรับระบบที่มีความสำคัญสูง จะต้องมีการตัดและหมดเวลาการใช้งาน โดยมีกำหนดให้ไม่เกิน ๑ ชั่วโมงต่อการพิสูจน์ตัวตนเข้าใช้งาน

๔. ต้องมีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบเทคโนโลยีสารสนเทศอีกครั้ง หลังจากที่ระบบได้หมดเวลาการใช้งานไปแล้ว

แนวปฏิบัติในการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๑.การจำกัดการเข้าถึงสารสนเทศ

ผู้ดูแลระบบต้องจากัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งาน ในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยมีวิธีการปฏิบัติ ดังนี้

๑. ผู้ดูแลระบบต้องป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วง โดยไม่ได้รับอนุญาต เช่น การใช้กุญแจล็อคที่ตัวเครื่อง การพิสูจน์ยืนยันตัวตน เป็นต้น

๒. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบ โดยกำหนดขั้นตอนและแบบฟอร์มการใช้งานระบบคอมพิวเตอร์ ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ชื่อผู้ใช้บริการ เหตุผลในการขอใช้ ระยะเวลาในการใช้บริการ

๓. ผู้ดูแลระบบต้องจำกัดระยะเวลาการเชื่อมต่อระบบ โดยตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานในช่วงเวลาที่กำหนด

๔. เจ้าของข้อมูลหรือเจ้าของระบบต้องกำหนดรายการข้อมูลสำหรับการให้บริการ ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง เป็นต้น

๕. เจ้าของข้อมูลหรือเจ้าของระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับสำหรับข้อมูลสำคัญ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) เวลาการใช้งานตั้งแต่ ๐๘.๓๐ – ๑๖.๓๐ น. และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้า รหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

(๕) ต้องกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) ต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของสำนักงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๖. มีการใช้เมนูเพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชันต่างๆ ของระบบงาน โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

๗. มีการลงทะเบียนผู้ใช้งาน เพื่อควบคุม จำกัด หรือให้สิทธิการเข้าถึงข้อมูลและฟังก์ชันต่างๆ ของระบบงาน เช่น การให้สิทธิในการอ่าน เขียน ลบ หรือสั่งให้โปรแกรมทำงาน โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

๘. มีการควบคุมหรือจำกัดสิทธิการเข้าถึงระบบงานซึ่งถูกเข้าถึงจากอีกระบบงานหนึ่ง โดยควบคุมให้สามารถเข้าถึงได้เฉพาะข้อมูลและฟังก์ชันต่างๆ ที่จำเป็นต้องใช้งานเท่านั้น

๙. มีการควบคุมหรือจำกัดการนำข้อมูลออกจากระบบงาน เพื่อให้สามารถเข้าถึงได้เฉพาะข้อมูลที่เกี่ยวข้องและจำเป็นสำหรับการนำไปใช้งานเท่านั้น

๑๐. มีการแสดงเฉพาะข้อมูลพื้นฐาน เพื่อให้ผู้ใช้งานได้รับทราบข้อมูลที่จำเป็นเท่านั้น

๑๑. มีการแสดงรายละเอียดเท่าที่จำเป็นของระบบงาน หลังจากที่ล็อกอินเสร็จแล้ว

๑๒. มีข้อความแสดงเตือน ห้ามผู้ไม่มีสิทธิเข้าถึงระบบงาน

๑๓. มีการตรวจสอบข้อมูลการล็อกอิน หลังจากที่ผู้ใช้งานใส่ข้อมูลทั้งหมดครบถ้วนแล้ว

๑๔. มีข้อจำกัดไม่ให้ระบบแสดงข้อความผิดพลาดจากการทำงานหรือการใช้งาน ในลักษณะที่เปิดเผยข้อมูลภายในของระบบงาน

๑๕. มีการจำกัดจำนวนครั้งที่ผู้ใช้งานสามารถใส่ข้อมูลการล็อกอินผิด

๑๖. มีการกำหนดการหน่วงระยะเวลาที่ผู้ใช้งานสามารถเชื่อมโยงกลับเข้ามายังระบบงานได้ ภายหลังจากที่ใส่ข้อมูลการล็อกอินผิดเกินกว่าจำนวนครั้งที่กำหนด

๑๗. มีการส่งข้อความเตือนไปยังผู้ดูแลระบบให้ทราบว่ามีผู้ใช้งานพยายามล็อกอินแต่ผิดพลาดเป็นจำนวนหลายครั้ง

๑๘. มีการบันทึกข้อมูลการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ

๑๙. มีการจำกัดช่วงระยะเวลาที่นานที่สุด ที่ผู้ใช้งานจะต้องล็อกอินเข้าใช้งานให้สำเร็จ

๒๐. มีการแสดงวันเวลาของการล็อกอินครั้งที่แล้ว (ทั้งที่สำเร็จและไม่สำเร็จ)

๒.ระบบที่ไวต่อการรบกวน

๑. ระบบเครือข่ายขององค์การ ในลักษณะที่ต้องวางผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้นั้น ต้องให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ การตัดสายสัญญาณเพื่อทำให้เกิดความเสียหายและป้องกันสัตว์ต่างๆ กัดสาย เช่น หนู เป็นต้น

๒. ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๓. จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

๔. ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๓.การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติอย่างเป็นทางการสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา อาทิ เครื่องคอมพิวเตอร์โน้ตบุ๊ก รวมทั้งกำหนดมาตรการการใช้งานอย่างปลอดภัยและเหมาะสม โดยมีแนวทางปฏิบัติดังนี้

๑. ต้องวิเคราะห์และประเมินความเสี่ยงจากลักษณะการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา

๒. สร้างความตระหนักเพื่อให้ผู้ใช้งานระมัดระวังและป้องกันการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น การใช้งานในที่สาธารณะ ห้องประชุม นอกสถานที่ ซึ่งรวมถึงการเชื่อมต่อผ่านทางเครือข่ายสาธารณะภายนอก สพภ. เป็นต้น

๓. ป้องกันข้อมูลที่จัดเก็บไว้ในอุปกรณ์ฯ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ด้วยการเข้ารหัสข้อมูล

๔. ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์ฯ

๕. สำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์ฯ อย่างสม่ำเสมอ

๖. ต้องควบคุมการเข้าถึงระบบงานของ สพภ. จากระยะไกล โดยการใช้อุปกรณ์คอมพิวเตอร์ประเภท

พกพา ซึ่งเชื่อมต่อผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตสาธารณะ

๗. ต้องระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย สำหรับการเข้าถึงระบบงานของ สพภ. จากระยะไกลโดยการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา

๘. ต้องควบคุมการติดตั้งโปรแกรมไม่พึงประสงค์ ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาของ สพภ.

๙. ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติ งาน เข้ามาปฏิบัติงานภายในห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ สพภ. จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาต เข้า - ออกพื้นที่ ให้ถูกต้องชัดเจน และต้องได้รับอนุญาตจากเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ด้วยการลงนามอย่างเป็นลายลักษณ์อักษร

๑๐. กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน โดยมีการจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ผู้เกี่ยวข้องรับทราบโดยทั่วกัน เช่น พื้นที่ติดตั้งอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless area) เป็นต้น

๔.การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๑. ต้องมีการกำหนดมาตรการและการเตรียมการต่าง ๆ ที่จำเป็นก่อน ซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๒. ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในองค์กร ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๓. ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์กร

๔. ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรในสถานที่ดังกล่าว

๕. ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร รวมทั้งมาตรการควบคุมการใช้เครือข่ายไร้สายที่บ้าน

๖. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ขององค์กรจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่องค์กรต้องการ

๗. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล

๘. องค์กรไม่อนุญาตให้ ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศ ขององค์กรจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยองค์กร

๙. องค์กรต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่าง ๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากระยะไกล

๑๐. องค์กรต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

๑.วิธีการบริหารจัดการการเข้าถึงของผู้ใช้งาน มีวิธีการปฏิบัติ ดังนี้

ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรใหม่ของสำนักงานกำหนดให้มีขั้น ตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆ ในการใช้งานตามความจำเป็น ต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศ ระบบงาน เครื่องคอมพิวเตอร์ที่ใช้งาน หรือเครื่องคอมพิวเตอร์พกพา โดยทันทีเมื่อเสร็จสิ้นงาน ต้องกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์ รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในสำนักงาน เป็นต้น

ขั้นตอนการลงทะเบียนเจ้าหน้าที่ใหม่ขององค์กร

๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศขององค์กร

๒) ผู้ดูแลระบบต้องตรวจสอบว่าผู้ใช้ได้รับมอบหมายสิทธิ์จากเจ้าของระบบสำหรับการใช้งานระบบสารสนเทศและบริการอย่างถูกต้อง ต้องมีการอนุมัติรับรองการได้สิทธิ์จากผู้บริหารอย่างชัดเจน

๓) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๔) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และมีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยขององค์กร

๕) ผู้ดูแลระบบต้องมอบเอกสารรับรองสิทธิ์การเข้าถึงแก่ผู้ใช้ เพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

๖) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยี สารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๗) การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

๘) การลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๘.๑ เจ้าหน้าที่ใหม่ขององค์กรกรอกข้อมูลคำขอใช้บริการลงแบบ ฟอร์มลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ เช่น คำขอใช้อินเตอร์เน็ต ระบบอีเมล์ หรือระบบงานต่าง ๆ

๘.๒ ยื่นคำขอกับผู้อำนวยการศูนย์สารสนเทศ หรือเจ้าหน้าที่ศูนย์สารสนเทศผู้ที่ได้รับมอบหมาย

๙) การให้สิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

๙.๑ ผู้ดูแลระบบตรวจสอบข้อมูลในแบบฟอร์ม ซึ่งข้อมูลจะต้องครบถ้วนทั้งหมด พร้อมทั้งต้องมีลายเซ็นของผู้ขอเข้าใช้งานระบบ ลายเซ็นของบุคคลผู้มีสิทธิ์อนุญาตในการลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๙.๒ ผู้ดูแลระบบตรวจสอบความซ้ำซ้อนของบัญชีผู้ใช้งาน

๙.๓ ผู้ดูแลระบบให้สิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม

๑๐) การแจ้งยกเลิกสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

๑๐.๑ หัวหน้างานหรือผู้บังคับบัญชา กรอกข้อมูลลงในแบบฟอร์ม และยื่นคำขอกับผู้อำนวยการศูนย์สารสนเทศ

๑๐.๒ ผู้ดูแลระบบยกเลิกสิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม และลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด

๒.วิธีการบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User account) และรหัสผ่าน มีวิธีการปฏิบัติ ดังนี้

๑. ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ที่รับผิดชอบ

๒. มีการกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน

๓. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

(๑) ต้องได้รับความเห็นชอบจากผู้ดูแลระบบงานนั้นๆ โดยนำเสนอผู้บังคับบัญชาอนุมัติ

(๒) ต้องควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ใช้งานเฉพาะกรณีที่จำเป็นเท่านั้น

(๓) ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

(๔) ต้องมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๓.วิธีการบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย มีวิธีการปฏิบัติ ดังนี้

(๑) กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

(๒) ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “๑๒๓๔๕”

(๓) ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

(๔) ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

(๕) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน ๓ ครั้ง

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านเครือข่ายคอมพิวเตอร์

(๗) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

(๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๔.วิธีการบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ มีวิธีการปฏิบัติ ดังนี้

๑. การจัดแบ่งประเภทของข้อมูล ประกอบด้วย

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลคำรับรอง ข้อมูลงบประมาณการเงินและบัญชี และข้อมูลระบบบริหารราชการ (Back Office)
- ข้อมูลสารสนเทศด้านการให้บริการ ได้แก่ ข้อมูลผู้รับบริการทางสังคม

๒. การจัดแบ่งระดับความสำคัญของข้อมูลแต่ละประเภทข้างต้น ดังนี้

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๓. การจัดแบ่งลำดับชั้นความลับของข้อมูลแต่ละประเภทข้างต้น ดังนี้

- ลับที่สุด
- ลับมาก

- ลับ

๔. การจัดแบ่งระดับชั้นการเข้าถึงข้อมูลแต่ละประเภทข้างต้น ดังนี้

- สามารถเข้าถึงได้เฉพาะผู้มีสิทธิสูงสุดในการบริหารจัดการระบบสารสนเทศ
- สามารถเข้าถึงได้เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิจากเจ้าของระบบงานแล้วเท่านั้น
- สามารถเข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง
- สามารถเข้าถึงได้โดยทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว

๕. การกำหนดเวลาการเข้าถึง ดังนี้

- การเข้าถึงสารสนเทศในเวลาราชการ (๐๘.๓๐ – ๑๖.๓๐ น.)
- การเข้าถึงสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา ๐๘.๓๐ – ๑๖.๓๐ น.)
- การเข้าถึงในช่วงเวลาวันหยุดราชการ (วันหยุดราชการ และวันหยุดนขัตฤกษ์)
- การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุช่วงการเข้าถึงและจำนวนระยะเวลาการเข้าถึง)

๖. การกำหนดจำนวนช่องทางที่สามารถเข้าถึงได้ ดังนี้

- ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)
- โทรศัพท์หรือโทรสาร (เข้าถึงได้ในเวลาราชการ)
- หนังสือหรือบันทึกข้อความ (เข้าถึงได้ในเวลาราชการ)
- ระบบแลน (เข้าถึงได้ทั้งในและนอกเวลาราชการ)
- ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)
- ระบบอินเตอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)
- ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)
- เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา หรือ ในช่วงเวลาพิเศษที่กำหนด)

ตารางสรุปแนวปฏิบัติในการเข้าถึงข้อมูลสารสนเทศของ สพภ. มีรายละเอียด ดังนี้

เวลาการเข้าถึง	ประเภทข้อมูลสารสนเทศ	ระดับความสาคัญ	ระดับชั้นการเข้าถึง	ระดับชั้นการเข้าถึง	ช่องทาง
การเข้าถึงสารสนเทศในเวลาราชการ (๐๘.๓๐ – ๑๖.๓๐ น.)	- ด้านการบริหาร - ด้านการให้บริการ	- มากที่สุด - ปานกลาง - น้อย	-	- เฉพาะกลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว	- ระบบแลน (LAN) - ระบบอินทราเน็ต (Intranet) - ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
การเข้าถึงสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา ๐๘.๓๐ –	- ด้านการบริหาร - ด้านการให้บริการ	- มากที่สุด - ปานกลาง - น้อย	-	- เฉพาะกลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว	- ระบบอินเทอร์เน็ต (Internet) - ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

๑๖.๓๐ น.)					
การเข้าถึงในช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนขัตฤกษ์)	- ด้านการบริหาร - ด้านการให้บริการ	- ปานกลาง - น้อย	-	- เฉพาะกลุ่มที่เกี่ยวข้อง - ทุกกลุ่มผู้ใช้ที่กำหนดไว้แล้ว	- ระบบอินเทอร์เน็ต (Internet) - ระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง (ระบุช่วงการเข้าถึงและจำนวนระยะเวลาการเข้าถึง)	- ด้านการบริหาร - ด้านการให้บริการ	- มากที่สุด	ลับที่สุด	- เฉพาะผู้มีสิทธิสูงสุดในการบริหารจัดการระบบสารสนเทศ - เฉพาะผู้ใช้ที่ได้รับอนุมัติสิทธิจากเจ้าของระบบงานแล้วเท่านั้น	- ระบบแลน (LAN) - ระบบอินทราเน็ต (Intranet)

แนวปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก หรือ Outsource

มีวิธีการปฏิบัติ ดังนี้

๑ ต้องมีการกำหนดมาตรการและการเตรียมการต่าง ๆ ที่จำเป็นก่อน ซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๒ ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในองค์กร ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๓ ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์กร

๔ ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรในสถานที่ดังกล่าว

๕ ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กร รวมทั้งมาตรการควบคุมการใช้เครือข่ายไร้สายที่บ้าน

๖ ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ขององค์กรจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่องค์กรต้องการ

๗ ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล

๘ องค์กรไม่อนุญาตให้ ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศ ขององค์กรจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยองค์กร

๙ องค์กรต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่าง ๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากระยะไกล

๑๐ องค์กรต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

ผู้ใช้งานเครือข่ายอินเตอร์เน็ตของสำนักงาน มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๑ การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเตอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเตอร์เน็ตของสำนักงาน โดยยื่นคำขอกับเจ้าหน้าที่กลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ โดยผู้ใช้งานต้องเป็นบุคลากรสังกัดสำนักงาน สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

๒ ไม่ใช้ระบบอินเทอร์เน็ตของสำนักงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับสำนักงาน

๓ ผู้ใช้งานอินเตอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

๔ ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่นการละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

๕ ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสำนักงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๖ ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นต้องดาว์นโหลดไฟล์ขนาดใหญ่ให้ปฏิบัตินอกเวลาทำงาน

๗ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสำนักงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสำนักงาน การทำลายความสัมพันธ์กับบุคลากรของสำนักงานอื่นๆ

แนวปฏิบัติในการใช้งานจดหมายอิเล็กทรอนิกส์

ผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของสำนักงานมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

๑. ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ ของสำนักงาน โดยยื่นคำขอกับเจ้าหน้าที่กลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ

๒. เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ควรเปลี่ยนรหัสผ่านโดยทันที

๓. ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้

๔. ควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

๕. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

๖. การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของสำนักงาน ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงานเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน ขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

๗. การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

๘. การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของสำนักงาน หรือก่อให้เกิดความเสียหายต่อสำนักงาน

๙. ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน เพื่อเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อการดำเนินงานของสำนักงาน ตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งผู้รับบริการของสำนักงาน

๑๐. การส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๑๑. การแนบไฟล์ข้อมูล สามารถแนบไฟล์ได้ไม่เกิน ๑๐ เมกะไบท์

๑๒. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ เสร็จสิ้นควรออกจากระบบ (Logout) ทุกครั้ง

แนวปฏิบัติในการจัดทำระบบสำรองข้อมูลและสารสนเทศ

๑. การสำรองข้อมูลและระบบคอมพิวเตอร์

ผู้ดูแลระบบหรือบุคลากรที่เกี่ยวข้อง จะต้องระบุแนวปฏิบัติสาหรับการจัดทาระบบสำรองข้อมูลที่ชัดเจน เพื่อให้ระบบสารสนเทศอยู่ในสภาพพร้อมใช้อยู่เสมอ โดยมีวิธีการปฏิบัติ ดังนี้

๑. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ ซึ่งดูแลรับผิดชอบระบบสารสนเทศ และระบบสำรองข้อมูลของสำนักงาน

๒. ผู้ดูแลระบบ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการจัดทำระบบสารองข้อมูลและสารสนเทศของสำนักงาน

๓. ทำการพิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นต้องจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้ตามลำดับความสำคัญ

๔. ระบบที่จะทำการสำรองข้อมูลต้องเป็นระบบที่มีความสำคัญต่อภารกิจของสำนักงาน

๕. มีการกำหนดประเภทของข้อมูลที่ต้องทำสำรองเก็บไว้ และความถี่ในการสำรอง

๖. จัดทำแผนการสำรองที่เหมาะสมกับความสำคัญของแต่ละระบบสารสนเทศ

๗. ดาเนินการตามกระบวนการสำรองข้อมูล สาหรับแต่ละระบบสารสนเทศโดยเคร่งครัด

๘. มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรอง ที่ใช้จัดเก็บข้อมูล

๙. การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก

๑๐. มีขั้นตอนปฏิบัติในการสำรองข้อมูลและกู้คืนข้อมูล แยกตามระบบสารสนเทศแต่ละระบบอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

๑๑. การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

๑๒. ให้มีการมอบหมายเจ้าหน้าที่สำรอง เพื่อทำหน้าที่สำรองข้อมูลในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้

๑๓. ในกรณีที่พบปัญหาในการสำรองข้อมูล จนเป็นเหตุให้ไม่สามารถดำเนินการได้อย่างสมบูรณ์ ให้ดำเนินการแก้ไขปัญหา สรุปผลการแก้ไขปัญหา และรายงานต่อผู้อำนวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ

๑๔. ให้ผู้ดูแลระบบ กำหนดชนิดและช่วงเวลาการสารองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๑๕. ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ (Backup Procedure) ตามนโยบายที่เกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) โดยเคร่งครัด

๒.การปฏิบัติเกี่ยวกับการสำรองข้อมูล มีวิธีการปฏิบัติ ดังนี้

๑. ผู้ดูแลระบบต้องทำการสำรองข้อมูลแต่ละรายการ โดยจะใช้วิธีสำรองข้อมูลแบบ Full Backup ตามความถี่ ดังนี้

(๑) Web servers : สำรองข้อมูลเผยแพร่บนเว็บไซต์ ๑ ครั้งต่อเดือน

(๒) Database servers : สำรองข้อมูลในฐานข้อมูลของระบบที่สาคัญ ๑ ครั้งต่อเดือน

(๓) Firewall server : สำรองข้อมูล Rule ของ Firewall ๑ ครั้งต่อเดือน

(๔) Server อื่นๆ : สำรองข้อมูลบนเซิร์ฟเวอร์อื่นๆ เช่น ระบบงานต่างๆ ๑ ครั้งต่อเดือน

๒. ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่า การสำรองข้อมูลตามรายละเอียดข้างต้นนั้น ถูกต้อง สมบูรณ์หรือไม่

๓. การทดสอบและการกู้คืนระบบ

ต้องกำหนดแผนการทดสอบกู้คืนข้อมูล ตามชนิดของการสำรองข้อมูลที่กำหนดไว้แล้ว เพื่อให้ระบบสารสนเทศมีสภาพพร้อมใช้งานอยู่เสมอ โดยมีวิธีการปฏิบัติ ดังนี้

๑. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่าย จนเป็นเหตุทำให้ต้องกู้คืนระบบ ผู้ดูแลระบบจะต้องดำเนินการแก้ไข พร้อมทั้งรายงานผลการแก้ไข บันทึก และสรุปผลการปฏิบัติงานต่อผู้อานวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายจากผู้อานวยการกลุ่มกิจการจัดการองค์ความรู้และเทคโนโลยีสารสนเทศทราบ

๒. การกู้คืนระบบ ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม

๓. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้ระบบทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดาเนินการเสร็จสิ้นอย่างสมบูรณ์

๔. กำหนดให้มีการทดสอบและปรับปรุงแผนการกู้คืนระบบ อย่างน้อยปีละ ๑ ครั้ง

๔.การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

สำนักงานต้องเตรียมการสำหรับจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง และต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจโดยมีวิธีการปฏิบัติ ดังนี้

๑. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ ซึ่งดูแลรับผิดชอบการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๒. ผู้ดูแลระบบจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินของระบบเทคโนโลยีสารสนเทศ เพื่อรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ

๓. ผู้ดูแลระบบต้องทดสอบ/ประเมิน และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้ หากเกิดเหตุการณ์ขึ้นจริง

๔. ผู้ดูแลระบบต้องบันทึกเหตุการณ์เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้น โดยพิจารณาถึง ประเภท ปริมาณ และหลักฐานสาหรับอ้างอิง เพื่อใช้ในกรณีที่เหตุการณ์มีความเกี่ยวข้องกับการดำเนินการทางกฎหมาย

๕. รายละเอียดที่ปรากฏในแผนเตรียมความพร้อมกรณีฉุกเฉิน ควรมีสาระครอบคลุมภัยพิบัติหรือสถานการณ์ฉุกเฉินที่มีผลกระทบต่อระบบสารสนเทศของสำนักงานโดยมีหัวข้อสำคัญ ดังนี้

- การเตรียมการเบื้องต้น
- ผู้รับผิดชอบ
- มาตรการความปลอดภัยและแผนดำเนินงาน ในการนำระบบคอมพิวเตอร์กลับสู่สภาพปกติเมื่อเกิดความเสียหายหรือหยุดทำงาน

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and assessment) อย่างน้อยปีละ ๑ ครั้ง โดยมีวิธีการปฏิบัติ ดังนี้

(๑) มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ

(๒) มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๓) มีการตรวจสอบและประเมินความเสี่ยงของระบบให้บริการ

(๔) มีการตรวจประเมินระบบสารสนเทศ (Information System Audit Considerations) อย่างน้อย ๑ ครั้งต่อปี เพื่อให้มั่นใจได้ว่าการตรวจประเมินมีประสิทธิภาพและผลการตรวจสอบเป็นที่น่าเชื่อถือได้

๒ การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบระบบสารสนเทศของ สพภ. (Internal IT Auditor) เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของ สพภ. โดยมีวิธีการปฏิบัติ ดังนี้

(๑) กำหนดให้หน่วยตรวจสอบภายใน ของ สพภ. เป็นผู้ตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศของ สพภ. และให้ตรวจสอบและประเมินความเสี่ยงอย่างน้อย ๑ ครั้งต่อปี

(๒) มีข้อตกลงร่วมกันสำหรับขอบเขตการตรวจสอบ ระหว่างผู้ตรวจสอบกับผู้รับการตรวจ

(๓) มีข้อจำกัดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ ในลักษณะที่อ่านได้เพียงอย่างเดียว

(๔) มีวิธีการที่ปลอดภัยสำหรับการอนุญาตให้ผู้ตรวจสามารถเข้าถึงข้อมูล ชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้

(๕) มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบทำงานบนข้อมูลสำเนา

(๖) มีการทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ

(๗) มีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจ

(๘) มีการกำหนดหน้าที่ความรับผิดชอบของผู้ตรวจสอบและขั้นตอนปฏิบัติสำหรับการตรวจสอบ

(๙) มีการกำหนดเจ้าหน้าที่ที่ทำหน้าที่เป็นผู้ตรวจสอบให้เป็นเอกเทศ จากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ (ผู้ตรวจสอบจะต้องไม่ตรวจสอบกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่ตนดูแลหรือรับผิดชอบ)

แนวปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. แนวทางปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑ จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของสำนักงาน

๒.๒ จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้

๒.๓ ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๒.๔ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ ได้ผ่านการพิจารณาจากคณะทำงานรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ ผู้กำกับดูแลด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง และให้เจ้าหน้าที่ทราบและถือปฏิบัติอย่างเคร่งครัดต่อไป

(นายสมเดช ชุนถนอม)
ผู้อำนวยการกลุ่มกิจการ
ปฏิบัติหน้าที่แทนรองผู้อำนวยการ
(กลุ่มภารกิจด้านยุทธศาสตร์ นวัตกรรม และองค์ความรู้)
ทำหน้าที่ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ
วันที่ .....๒๑ ก.ค. ๕๘.....