นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
กรมพัฒนาฝีมือแรงงาน

๑. หลักการและเหตุผล

กรมพัฒนาฝีมือแรงงาน ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานตามภารกิจของกรมพัฒนาฝีมือแรงงาน เช่น ระบบฝึกอบรมฝีมือแรงงาน ระบบทดสอบมาตรฐานฝีมือแรงงาน ระบบรับรองความรู้ความสามารถ และระบบการให้บริการประชาชนและสถานประกอบกิจการ ซึ่งการพัฒนาระบบต้องใช้ระยะเวลาและการลงทุนสูง โดยองค์ประกอบหลักของระบบเทคโนโลยีสารสนเทศประกอบด้วยฮาร์ดแวร์และซอฟต์แวร์รวมทั้งระบบเครือข่ายที่มีการเชื่อมต่อกันทั้งภายในและภายนอก ระบบต้องมีความสะดวก รวดเร็ว ง่ายต่อการเข้าถึงซึ่งก็เป็นผลเชิงบวกของเทคโนโลยีที่อำนวยความสะดวกให้กับการดำเนินงานราชการในยุคปัจจุบันจากความสะดวกสบายนี้เองที่ทำให้มีภัยคุกคามที่อยู่ในวงกว้าง ซึ่งภัยเหล่านี้อาจก่อให้เกิดความเสียหายต่องานราชการหรือองค์กรได้ จึงต้องมีการดูแลรักษาระบบให้สามารถใช้งานได้ตลอดเวลาในขณะเดียวกันระบบเทคโนโลยีสารสนเทศเป็นสินทรัพย์ที่สำคัญสำหรับการดำเนินงานราชการและเป็นสิ่งที่มีค่ายิ่งสำหรับองค์กรจึงจำเป็นต้องได้รับการป้องกันรักษาเช่นเดียวกับสินทรัพย์อื่น

ทั้งนี้ เพื่อเป็นการป้องกันเชิงรุกต่อความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคาม และอีกทั้งถือเป็นนโยบายและหลักการปฏิบัติเพื่อให้เกิดความมั่นคงปลอดภัย ความน่าเชื่อถือ ต่อระบบเทคโนโลยีสารสนเทศ กรมพัฒนาฝีมือแรงงานจึงได้ศึกษาเป้าหมายแนวทางการดำเนินการ และได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมพัฒนาฝีมือแรงงาน เป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่อง และป้องกันภัยคุกคามต่าง ๆ และการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่าง ๆ ด้วย

๒. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรม หรือต่อไปนี้เรียกว่า “องค์กร” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ องค์กรจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพ และประสิทธิผล

๒.๒ นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบ และเจ้าหน้าที่ทุกคนจะต้องยอมรับ และปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงาน และปฏิบัติตามอย่างเคร่งครัด

๒.๔ นโยบายนี้ต้องมีการดำเนินการตรวจสอบ และประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

๓. องค์ประกอบของนโยบาย

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมพัฒนาฝีมือแรงงาน จัดทำขึ้นเพื่อกำหนดแนวทาง และวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ และมาตรา ๙ ที่กำหนดให้หน่วยงานภาครัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีสาระสำคัญดังนี้

๓.๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

๓.๒ นโยบายการสำรองข้อมูลและการกู้คืนข้อมูล

๓.๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๔. การเผยแพร่และทบทวน

นโยบายความมั่นคงปลอดภัยสารสนเทศของกรมพัฒนาฝีมือแรงงานฉบับนี้ จะได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศกรมพัฒนาฝีมือแรงงาน และมีการจัดพิมพ์เผยแพร่เพื่อให้เจ้าหน้าที่ของกรมพัฒนาฝีมือแรงงานของบุคคลภายนอกที่เกี่ยวข้องได้ทราบ และถือปฏิบัติตามนโยบายนี้ อย่างเคร่งครัด

คำนิยามและความหมาย

๑. องค์กร หมายถึง กรมพัฒนาฝีมือแรงงาน

๒. เครือข่ายคอมพิวเตอร์ หมายถึง เครือข่ายคอมพิวเตอร์ของกรมพัฒนาฝีมือแรงงาน

๓. ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารราชการของกรมพัฒนาฝีมือแรงงาน

๔. ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม (Department Chief Information Officer : DCIO) หมายถึง ผู้บริหารของกรมที่รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารในองค์กร

๕. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ซึ่งมีบทบาทหน้าที่ และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

๖. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายภายในองค์กร

๗. การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมพัฒนาฝีมือแรงงาน

๘. มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติงานเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

๙. แนวปฏิบัติ หมายถึง แนวที่ต้องปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายของนโยบาย

๑๐. แนวนโยบาย หมายถึง หลักการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการทำธุรกรรมอิเล็กทรอนิกส์ที่กรมพัฒนาฝีมือแรงงาน ซึ่งประกาศไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานที่เกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นในแนวทางเดียวกัน

๑๑. ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของกรมพัฒนาฝีมือแรงงาน โดยมีอำนาจหน้าที่ตามที่กรมพัฒนาฝีมือแรงงานกำหนด ดังนี้

๑๑.๑ ผู้ดูแลระบบเครือข่าย หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงแอปพลิเคชันเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

๑๑.๒ ผู้ดูแลเครื่องแม่ข่าย หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบแม่ข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงเครื่องแม่ข่าย ทรัพยากรแม่ข่าย เพื่อการจัดการข้อมูลหรือการตั้งค่าของเครื่องแม่ข่ายคอมพิวเตอร์

๑๑.๓ ผู้พัฒนาระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการพัฒนาระบบแอปพลิเคชัน

๑๑.๔ เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ และเจ้าหน้าที่ประจำโครงการขององค์กร

๑๑.๕ บุคคลภายนอก หมายถึง บุคคลที่กรมพัฒนาฝีมือแรงงานอนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศของกรมพัฒนาฝีมือแรงงานได้ชั่วคราวเพื่อประโยชน์ในการดำเนินงานของกรมพัฒนาฝีมือแรงงาน เช่น พนักงานหรือลูกจ้างบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบให้กับกรมพัฒนาฝีมือแรงงาน หรือที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้างหรือนิสิตนักศึกษาฝึกงาน

๑๒. สิทธิ หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๑๓. สินทรัพย์ (Asset) หรือทรัพย์สินสารสนเทศ หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร อันได้แก่

๑๓.๑ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

๑๓.๒ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด

๑๓.๓ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

๑๔. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control) หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ เข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๑๕. ความมั่นคงปลอดภัยด้านสารสนเทศ/ระบบสารสนเทศ (Information Security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึงการป้องกันทรัพย์สินสารสนเทศจากการเข้าถึงใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้โดยมิชอบ

๑๖. หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานที่กรมพัฒนาฝีมือแรงงานอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูล หรือสินทรัพย์ต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๗. ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๘. สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ โดยในที่นี้เรียกรวมว่า “ข้อมูล”

๑๙. ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๒๐. ระบบเครือข่าย หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์สื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของกรมพัฒนาฝีมือแรงงานได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet)

๒๑. ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย แอปพลิเคชันข้อมูลและสารสนเทศ เป็นต้น

๒๒. เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๒๓. รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตรวจตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๒๔. ชุดคำสั่งไม่พึงประสงค์ (Malicious Software) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๒๕. ห้องคอมพิวเตอร์แม่ข่าย หมายถึง ห้องคอมพิวเตอร์ และระบบเครือข่าย ในการสนับสนุนการให้บริการด้านเทคโนโลยีสารสนเทศ

๒๖. ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and environment security) หมายถึง การจัดให้มีนโยบาย มาตรการหลักเกณฑ์ หรือกระบวนการใด ๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์อื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

๒๗. ผู้ตรวจสอบระบบสารสนเทศภายในของหน่วยงาน (Internal IT Auditor) หมายถึง ผู้ที่ได้รับมอบหมายจากอธิบดีกรมพัฒนาฝีมือแรงงาน ให้มีหน้าที่ตรวจสอบเกี่ยวกับระบบสารสนเทศของกรมพัฒนาฝีมือแรงงาน

นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ
(Access Control Policy)

๑. วัตถุประสงค์

๑.๑ เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึง และการใช้งานระบบสารสนเทศของหน่วยงาน

๑.๒ เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงาน ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบเครือข่าย

๓. แนวปฏิบัติ

ในด้านการรักษาความมั่นคงปลอดภัย แนวปฏิบัติที่สอดคล้อง กับนโยบายการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ ของกรมพัฒนาฝีมือแรงงาน ดังนี้

ส่วนที่ ๑ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical and environment security)

ส่วนที่ ๒ แนวปฏิบัติการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่าย
(Computer Center Entry Control)

ส่วนที่ ๓ แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Access Control)

ส่วนที่ ๔ แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Third party access control)

ส่วนที่ ๕ แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา
(Use of Personal Computer and Notebook computer)

ส่วนที่ ๖ แนวปฏิบัติการใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์
(Use of the Internet and Social Network)

ส่วนที่ ๗ แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

ส่วนที่ ๘ แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control)

ส่วนที่ ๙ แนวปฏิบัติการกำหนดผู้รับผิดชอบ
(responsible)

ส่วนที่ ๑๐ แนวปฏิบัติการควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย
(Firewall Access Control)

ส่วนที่ ๑๑ แนวปฏิบัติการรับมือเหตุภัยคุกคามทางไซเบอร์
(cybersecurity incident response plan

ส่วนที่ ๑
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical and environment security)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบเครือข่าย

๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๓.๑ ภายในองค์กร ควรมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม โดยจัดทำเป็นเอกสาร "การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ" เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๓.๒ ผู้ดูแลระบบเครือข่าย ควรกำหนด และแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน และประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

๓.๓ ผู้ดูแลระบบเครือข่าย ต้องกำหนดสิทธิ์ให้กับเจ้าหน้าที่ ให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

๓.๓.๑ จัดทำ "ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่" เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓ ๓ ๒ ทำการบันทึกการเข้าออกพื้นที่ใช้งาน และกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร "บันทึกการเข้าออกพื้นที่"

๓.๓.๓ ควรมีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ ๑ ครั้ง

๔. การควบคุมการเข้าออก อาคาร สถานที่

๔.๑ ในการเข้าถึงสถานที่ มีขั้นตอนในการดำเนินการ ดังนี้

๔.๑.๑ การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ

๔.๑.๒ บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อตรงจุดที่สามารถเห็นได้ชัดเจน ตลอดเวลาที่อยู่ในองค์กร

๔.๑.๓ กรณีที่บุคคลภายนอกหรือผู้ติดต่อ ต้องการนำอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์พกพา หรืออุปกรณ์เครือข่ายเข้าบริเวณอาคาร เจ้าหน้าที่รักษาความปลอดภัยจะต้องลงบันทึกในแบบฟอร์มการเข้าออกในรายการอุปกรณ์ที่นำเข้ามาให้ถูกต้อง

๔.๑.๔ บุคคลภายนอกหรือผู้ติดต่อ จะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกได้ถูกต้อง

๔.๑.๕ บุคคลภายนอกหรือผู้ติดต่อ ต้องคืนแบบฟอร์มการเข้าออกและบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และเจ้าหน้าที่รักษาความปลอดภัย. ต้องตรวจสอบผู้ติดต่อ อุปกรณ์พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

๔.๒ จะได้รับสิทธิ์ให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๔.๓ หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้งานระบบ ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ ต้องตรวจสอบเหตุผล และความจำเป็น ก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่องค์กรออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคล และการขอเข้าออกไว้เป็นหลักฐานทั้งในกรณีที่อนุญาต และไม่อนุญาตให้เข้าพื้นที่

ส่วนที่ ๒
แนวปฏิบัติการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่าย
(Server Room Entry Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลขององค์กร โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องศูนย์คอมพิวเตอร์

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบเครือข่าย

๓. คำจำกัดความของผู้เกี่ยวข้อง

๓.๑ ผู้ดูแลระบบเครือข่าย หมายถึง เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการ และบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓.๒ เจ้าหน้าที่ หมายถึง เจ้าหน้าที่องค์กรที่มีสิทธิ์ในการเข้าออกสถานที่ อาหาร ห้อง ภายในองค์กร

๓.๓ ผู้ติดต่อจากหน่วยงานภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่มาทำการติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๔. บทบาทและความรับผิดชอบ

ผู้ดูแลระบบเครือข่าย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่ดังนี้

๑) ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสารให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อย่างเคร่งครัด

๒) ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องติดบัตรผู้ติดต่อหรือบัตรประจำตัวขององค์กร เท่านั้น

๕. กระบวนการควบคุมการเข้าออกห้องศูนย์คอมพิวเตอร์

๕.๑ ผู้ดูแลระบบเครือข่าย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และเจ้าหน้าที่ ขององค์กรมีแนวทางปฏิบัติ ดังนี้

๕.๑.๑ ผู้ดูแลระบบเครือข่าย ควรจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่นส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) ส่วนเครื่องพิมพ์ (Printer Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงาน และยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

๕.๑.๒ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกห้องคอมพิวเตอร์แม่ข่าย โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

๕.๑.๓ ต้องจัดทำระบบเก็บบันทึกการเข้าออกห้องคอมพิวเตอร์แม่ข่าย ตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

๕.๑.๔ กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออกห้องคอมพิวเตอร์แม่ข่าย ก็ต้องมีการควบคุมอย่างรัดกุม

๕.๑.๕ การเข้าออกห้องคอมพิวเตอร์แม่ข่าย ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

๕.๑.๖ เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทุกคนต้องตรวจสอบให้มั่นใจบุคคลที่ผ่านเข้าออกทุกคนต้องกรอกแบบฟอร์มดังกล่าว

๕.๒ ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติดังนี้

๕.๒.๑ ผู้ติดต่อจากหน่วยงานภายนอก ทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

๕.๒.๒ ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในองค์กร จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน

๕.๒.๓ ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๕.๒.๔ ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าออกศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้ด้วยบัตรผู้ติดต่อโดยสิทธิ์จะขึ้นอยู่กับเหตุผลความจำเป็นในการขอเข้าปฏิบัติงานภายในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๕.๒.๕ พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้าออก และต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

๕.๒.๖ ผู้ติดต่อจากหน่วยงานภายนอก ต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัย ซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตร และตรวจสอบแบบฟอร์มการขออนุญาตเข้าออกว่ามีเจ้าหน้าที่ลงนามอนุญาตแล้วทุกครั้ง

๕.๒.๗ เจ้าหน้าที่รักษาความปลอดภัย ต้องตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในแบบฟอร์มการขออนุญาตเข้าออก และตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง

๕.๒.๘ ผู้ดูแลระบบเครือข่าย ต้องทำการทบทวนสิทธิ์ของเจ้าหน้าที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ ๒ ครั้ง

ส่วนที่ ๓
แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบสารสนเทศ

๒.๓ ผู้ดูแลระบบเครือข่าย

๒.๔ ผู้ดูแลเครื่องแม่ข่าย

๓. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

๓.๑ สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์ และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๓.๒ ผู้ดูแลระบบสารสนเทศ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓.๓ ผู้ดูแลระบบสารสนเทศ หรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

๓.๔ ผู้ดูแลระบบเครือข่าย ควรจัดให้มีการติดตั้งระบบบันทึก และติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร หรือระบบจัดเก็บ log ไฟล์ ในองค์กร เพื่อตรวจสอบการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลสำคัญ

๓.๕ ผู้ดูแลระบบเครือข่าย ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๔. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๔.๑ ผู้ดูแลระบบสารสนเทศ มีหน้าที่ในการตรวจสอบการอนุมัติ และกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ได้แก่ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

๔.๒ เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้เข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

๔.๓ จะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูล และระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๕. การบริหารจัดการการเข้าถึงของผู้ใช้

๕.๑ การลงทะเบียนเจ้าหน้าที่ใหม่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในองค์กร เป็นต้น

๕.๒ กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๕.๓ ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

๕.๔ การบริหารจัดการบัญชีรายชื่อ และรหัสผ่านของเจ้าหน้าที่

๕.๔.๑ ผู้ดูแลระบบสารสนเทศ ที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ ซึ่งมีแนวทางปฏิบัติ ตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๕.๔.๒ การกำหนด การเปลี่ยนแปลง และการยกเลิกรหัสผ่าน ต้องปฏิบัติตาม “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

๕.๔.๓ กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานระบบ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

๑) ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ

๒) ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๔) ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๕.๕ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๕.๕.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๕.๕.๒ เจ้าของข้อมูล จะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลของเหล่านี้อย่างน้อยปีละ ๔ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๕.๕.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบ ต้องกำหนดรายชื่อและรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

๕.๕.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

๕.๕.๕ ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล ตามที่ระบุไว้ในเอกสาร "การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน"

๕.๕.๖ ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ขององค์กร เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรอง และลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๖. การบริหารจัดการการเข้าถึงระบบเครือข่าย

๖.๑ ผู้ดูแลระบบเครือข่าย ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๖.๒ การเข้าสู่ระบบเครือข่ายภายในขององค์กร โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อนที่จะสามารถใช้งานได้ในทุกกรณี

๖.๓ ผู้ดูแลระบบเครือข่ายต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๖.๔ ระบบเครือข่ายทั้งหมดขององค์กรที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกองค์กร ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจสอบมัลแวร์ ด้วย

๖.๕ ผู้ดูแลระบบเครือข่ายต้องมีการติดตั้งระบบตรวจจับการบุกรุก เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายขององค์กรในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๖.๖ การเข้าสู่ระบบงานเครือข่ายภายในองค์กร โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตนเพื่อตรวจสอบความถูกต้อง

๖.๗ IP address ภายในของระบบงานเครือข่ายภายในขององค์กร จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่าย และส่วนประกอบของศูนย์เทคโนโลยีสารสนเทศได้โดยง่าย

๖.๘ ผู้ดูแลระบบเครือข่ายต้องจัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๖.๙ การติดตั้ง และการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

๗. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๗.๑ ผู้ดูแลเครื่องแม่ข่าย ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่ายในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบอย่างชัดเจน

๗.๒ ผู้ดูแลเครื่องแม่ข่าย ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

๗.๓ ผู้ดูแลเครื่องแม่ข่าย ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet ftp หรือ ping เป็นต้น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

๗.๔ ผู้ดูแลเครื่องแม่ข่าย ควรดำเนินการติดตั้งอัปเดตระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมหรือระบบอย่างสม่ำเสมอ เช่น Web Server เป็นต้น

๗.๕ ผู้ดูแลเครื่องแม่ข่าย ควรดำเนินการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) สำหรับเครื่องแม่ข่ายและอัพเดทซอฟต์แวร์ให้เป็นปัจจุบัน เพื่อป้องกันความเสี่ยงจากไวรัส หรือมัลแวร์ที่เข้ามาโจมตีเครื่องแม่ข่าย

๗.๖ ควรมีการทดสอบโปรแกรมระบบ เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้ง และหลังจากการแก้ไขหรือบำรุงรักษา

๗.๗ การติดตั้ง และการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

๗.๘ ควรจะมีการสำรองไฟล์หรือข้อมูลตั้งค่า (Configuration) ของเครื่องแม่ข่าย เพื่อป้องกันข้อมูลสูญหาย ในกรณีที่เกิดความเสียหายกับระบบ

๘. การบริหารจัดการการบันทึกและตรวจสอบ

๘.๑ ควรกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่าย และเครือข่ายบันทึกการปฏิบัติงานของ (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๘.๒ ควรมีการตรวจสอบบันทึกการปฏิบัติงานของอย่างสม่ำเสมอ

๘.๓ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๙. การควบคุมการเข้าใช้งานระบบจากภายนอก

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

๙.๑ การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กร ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูล และทรัพยากรขององค์กร การควบคุมบุคคลที่เข้าสู่ระบบขององค์กรจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๙.๒ วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบ และข้อมูลอย่างเคร่งครัด

๙.๓ ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๙.๔ ต้องมีการควบคุมพอร์ต ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้าองค์กรนั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบ และวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๙.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๑๐. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

๑๐.๑ ผู้ใช้ระบบทุกคนเมื่อจะเข้าใช้งานระบบ ต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร สำหรับในทางปฏิบัติจะแบ่งออกเป็นสองขั้นตอน คือ

๑๐.๑.๑ การแสดงตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงชื่อผู้ใช้ (Username)

๑๐.๑.๒ การพิสูจน์ยืนยันตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นผู้ใช้ตัวจริง เช่น การใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ดหรือการใช้ USB token ที่มีความสามารถ PKI เป็นต้น

๑๐.๒ การเข้าสู่ระบบสารสนเทศขององค์กรนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย ๑ วิธี

๑๐.๓ การเข้าสู่ระบบสารสนเทศขององค์กรจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบด้วย

๑๐.๔ การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของ เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

ส่วนที่ ๔
แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Third party access control)

๑. วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรให้เป็นไปอย่างมั่นคงปลอดภัย และกำหนดแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบการใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบเครือข่าย

๓. แนวทางปฏิบัติ

๓.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารได้

๓.๒ การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

๓.๒.๑ บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กรจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓.๒.๒ จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

๑) เหตุผลในการขอใช้

๒) ระยะเวลาในการใช้

๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

๔) การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

๕) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๓.๒.๓ หน่วยงานภายนอก ที่ทำงานให้กับองค์กรทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๓.๒.๔ องค์กร ควรพิจารณาการเข้าไปประเมินความเสี่ยงหรือจัดทำการควบคุมภายในของหน่วยงานภายนอก ทั้งนี้ ขึ้นอยู่กับความสำคัญของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เข้าไปปฏิบัติงาน

๓.๒.๕ เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

๓.๒.๖ สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญขององค์กร ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ การรักษาความถูกต้องของข้อมูล และการรักษาความพร้อมที่จะให้บริการ

๓.๒.๗ องค์กรมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจว่า องค์กรสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

๓.๒.๘ ควรดำเนินการให้ผู้ให้บริการหน่วยงานภายนอกจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

ส่วนที่ ๕
แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา
(Use of Personal Computer and Notebook computer)

๑. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพานี้ ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่ และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ขององค์กร และผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากร และข้อมูลที่มีค่าขององค์กร ให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบเครือข่าย

๒.๓ ผู้ใช้งาน

๓. การใช้งานทั่วไป

๓.๑ เครื่องคอมพิวเตอร์ที่องค์กรอนุญาตให้ผู้ใช้ ใช้งานเป็นทรัพย์สินขององค์กร ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานขององค์กร

๓.๒ ห้ามคัดลอกโปรแกรมลิขสิทธิ์ที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ขององค์กรไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓.๓ การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ ตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่านั้น

๓.๔ ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๓.๕ ไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

๓.๖ ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ เป็นต้น

๓.๗ การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๓.๘ ผู้ใช้งานไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๓.๙ มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยควรปฏิบัติ ดังนี้

๓.๙.๑ ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

๓.๙.๒ ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Hard Disk Drive

๓.๙.๓ ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหายของคอมพิวเตอร์ เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๔. การควบคุมการเข้าถึงระบบปฏิบัติการ

๔.๑ ต้องกำหนดชื่อ (User name) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

๔.๒ ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ โดยตั้งเวลาประมาณ ๑๐ นาที เพื่อให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

๔.๓ ไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อ (User name) และรหัสผ่าน (Password) ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๔.๔ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ควร Logout ออกจากเครื่องคอมพิวเตอร์ หรือล็อกหน้าจอด้วยโปรแกรม Screen Saver

๕. แนวทางปฏิบัติในการใช้รหัสผ่าน

ให้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร "การบริหารจัดการสิทธิ์การใช้งานระบบ และรหัสผ่าน"

๖. การป้องกันเครื่องคอมพิวเตอร์จากโปรแกรมไวรัสคอมพิวเตอร์

๖.๑ ต้องทำการ Update ระบบปฏิบัติการ เว็บเบราว์เซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๖.๒ ต้องติดตั้งและ Update โปรแกรมป้องกันไวรัส อย่างสม่ำเสมอ เพื่อป้องกันความเสี่ยงจากไวรัสหรือมัลแวร์ ที่เข้ามาโจมตีเครื่องคอมพิวเตอร์

๖.๓ ควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น CD, DVD, Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

๖.๔ ผู้ใช้งานควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

๖.๕ ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๗. การสำรองข้อมูลและการกู้คืน

๗.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

๗.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๗.๓ ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการขององค์กร

ส่วนที่ ๖
แนวปฏิบัติการใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์
(Use of the Internet and Social Network)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์อย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ขององค์กรถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบเครือข่าย

๒.๓ ผู้ใช้งาน

๓. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

๓.๑ ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่องค์กรจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IP-IDS เป็นต้น

๓.๒ เครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่

๓.๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

๓.๔ ผู้ใช้งานต้องไม่ใช้เครือข่ายอินเทอร์เน็ตขององค์กร เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๓.๕ ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่าย และความปลอดภัยทางข้อมูลขององค์กร

๓.๖ ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับองค์กร

๓.๗ ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานขององค์กร ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๓.๘ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์คอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๓.๙ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้ จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๓.๑๐ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้อง และความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๓.๑๑ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๓.๑๒ การใช้งานเว็บบอร์ดขององค์กร ผู้ใช้ต้องไม่เปิดเผยข้อมูลที่สำคัญ และเป็นความลับขององค์กร

๓.๑๓ ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงขององค์กร การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

๓.๑๔ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

๔. แนวทางปฏิบัติในการใช้งานเครือข่ายสังคมออนไลน์

๔.๑ การสร้างบัญชีและการใช้งานสื่อสังคมออนไลน์ โดยต้องพิจารณาถึง การตั้งค่าความเป็นส่วนตัว (Privacy Setting) การรักษาความปลอดภัยของบัญชีสื่อสังคมออนไลน์เพื่อป้องกันการเข้าใช้โดยไม่ได้รับอนุญาต

๔.๒ ผู้ใช้งานต้องไม่สร้างหรือใช้งานบัญชีสื่อสังคมออนไลน์ที่ทำการปลอมแปลงขึ้นเพื่อให้บุคคลภายนอกเชื่อว่าเป็นบัญชีสื่อสังคมออนไลน์ของกรม ไม่ว่าจะเป็นการใช้ชื่อ หรือรูปสัญลักษณ์ของกรมอันก่อให้เกิดความเสียหายแก่กรม หรือนำไปแสวงหาประโยชน์เพื่อตนเองหรือบุคคลภายนอก

๔.๓ การใช้งานสื่อสังคมออนไลน์ จะต้องเป็นไปตามกฎหมายที่เกี่ยวข้องอย่างเคร่งครัด เช่น ประมวลกฎหมายอาญาว่าด้วยความผิดฐานหมิ่นประมาท พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ และพระราชบัญญัติลิขสิทธิ์ พ.ศ.๒๕๓๗ เป็นต้น

๔.๔ การใช้งานสื่อสังคมออนไลน์จะต้องไม่เผยแพร่ข้อมูลข่าวสารที่เป็นข้อมูลความลับหรือข้อมูลที่เกี่ยวข้องกับความปลอดภัยของกรมรวมถึงข้อมูลที่เป็นเท็จอันอาจก่อให้เกิดความเสียหาย กระทบถึงภาพลักษณ์ และการดำเนินการของกรม

๔.๕ การใช้งานสื่อสังคมออนไลน์ จะต้องไม่แสดงสัญลักษณ์ทางการเมืองพรรคการเมือง กลุ่มการเมือง กลุ่มเคลื่อนไหวกดดัน ที่แสดงถึงความไม่เป็นอิสระ ไม่เป็นกลาง หรือก่อให้เกิดความเข้าใจผิดแก่สังคมหรือบุคคลภายนอก รวมทั้งข้อมูลที่เกี่ยวกับความมั่นคงของประเทศ หรือกระทบต่อสถาบันพระมหากษัตริย์

๔.๖ การใช้งานสื่อสังคมออนไลน์ของกรม จะต้องไม่ใช้ในการประกอบธุรกิจการค้าหรือใช้งานในเชิงพาณิชย์เพื่อประโยชน์ของพนักงานหรือของบุคคลภายนอก

ส่วนที่ ๗
แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร ซึ่งผู้ใช้จะต้องให้ความสำคัญ และตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์

๒.๓ ผู้ใช้งาน

๓. แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

๓.๑ ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ขององค์กร ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

๓.๒ ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ขององค์กร

๓.๓ สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรก ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

๓.๔ การกำหนดรหัสผ่านที่ดี (Good Password) มีแนวทางปฏิบัติตามที่ระบุไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบ และรหัสผ่าน

๓.๕ ผู้ใช้งานไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติของระบบจดหมายอิเล็กทรอนิกส์

๓.๖ ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

๓.๗ ผู้ใช้งานควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อองค์กรหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายขององค์กร

๓.๘ ข้อห้าม ผู้ใช้งานไม่ควรใช้ e-mail address ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๓.๙ ผู้ใช้งานควรใช้ e-mail address ขององค์กร เพื่อการทำงานขององค์กรเท่านั้น

๓.๑๐ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๓.๑๑ ผู้ใช้งานควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น

๓.๑๒ ผู้ใช้งานไม่เปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๓.๑๓ ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงขององค์กร ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์

๓.๑๔ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๓.๑๕ ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๓.๑๖ ผู้ใช้งานควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๓.๑๗ ข้อควรระวัง ผู้ใช้งานไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ส่วนที่ ๘
แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ขององค์กร โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบเครือข่าย

๒.๓ ผู้ใช้งาน

๓. แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๓.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายขององค์กร จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารอย่างเป็นลายลักษณ์อักษร

๓.๒ ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓.๓ ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๓.๔ ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น

๓.๕ ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

๓.๖ ผู้ดูแลระบบควรเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและผู้ดูแลระบบควรเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดา หรือเจาะรหัสได้โดยง่าย

๓.๗ ผู้ดูแลระบบต้องกำหนดค่าใช้ Web หรือ WPA ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากขึ้น

๓.๘ ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

๓.๙ ผู้ดูแลระบบควรจะมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในองค์กร

๓.๑๐ ผู้ดูแลระบบ ควรกำหนดให้ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

๓.๑๑ ผู้ดูแลระบบ ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบ และบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

ส่วนที่ ๙
แนวปฏิบัติการกำหนดผู้รับผิดชอบ
(responsible)

๑. วัตถุประสงค์

เพื่อกำหนดหน้าที่ความรับผิดชอบของผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม ผู้อำนวยการ หัวหน้า เจ้าหน้าที่ ตลอดจนผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบด้านสารสนเทศ

๒. ผู้รับผิดชอบ

๒.๑ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO)

๒.๒ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๓ ผู้ดูแลระบบ

๓. แนวทางปฏิบัติระดับนโยบาย

๓.๑ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือบุคคลใดบุคคลหนึ่ง อันเนื่องมาจากความบกพร่องละเลยหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO)เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๓.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงาน และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ติดตาม และกำกับดูแลควบคุมตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติ

๔. แนวทางปฏิบัติระดับผู้บริหาร

๔.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงานอย่างใกล้ชิด ให้ความเห็น เสนอแนะวิธีการ และแนวทางการแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบฐานข้อมูล และสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคง และความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการรวมทั้งรับผิดชอบ ดังนี้

๔.๑.๑ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ Sever และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง

๔.๑.๒ แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยง และความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ และระบบเครือข่ายของกรม

๔.๑.๓ กำกับดูแล เกี่ยวกับสารสนเทศ และงานต่าง ๆ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๔.๑.๔ รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่าย และระบบฐานข้อมูลสารสนเทศ ให้แก่ผู้บังคับบัญชาระดับสูงทราบสม่ำเสมอ

๕. แนวทางปฏิบัติระดับปฏิบัติ

ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการกรม เช่น นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่เครื่องคอมพิวเตอร์

๕.๑ ปฏิบัติตามนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕.๒ ประสานการปฏิบัติงานตามแผนป้องกัน และแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอน และภัยพิบัติ

๕.๓ รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย

๕.๔ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๕.๕ ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจาก บุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๕.๖ รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต

๕.๗ ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรม

ส่วนที่ ๑๐
แนวปฏิบัติการควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย
(Firewall Control)

๑. วัตถุประสงค์

เพื่อป้องกันการโจมตีการรักษาความปลอดภัยเครือข่าย หรือการโจมตีของแฮกเกอร์ ไฟร์วอลล์ฮาร์ดแวร์สามารถกำหนดค่าหรือกฎเฉพาะที่สามารถจดจำและบล็อคไวรัสและมัลแวร์ได้ และยังสามารถบล็อคการเข้าถึงจากภายนอกที่ไม่ได้รับอนุญาตอีกด้วย

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบเครือข่าย

๒.๓ ผู้ดูแลเครื่องแม่ข่าย

๓. แนวทางปฏิบัติในการควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย

๓.๑ หน่วยงานมีหน้าที่ในการบริหารจัดการ การติดตั้งและกำหนดค่าของ Firewall ทั้งหมด

๓.๒ การกำหนดค่าเริ่มต้นของ Firewall ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

๓.๓ ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเตอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้องถูกบล็อก (Block) โดย Firewall

๓.๔ ผู้ใช้งานอินเตอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนการใช้งานทุกครั้ง

๓.๕ การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง หากมีการเปลี่ยนแปลงค่าต่าง ๆ ของ Firewall

๓.๖ การเข้าถึงตัวอุปกรณ์ Firewall จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการ

๓.๗ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ Firewall จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

๓.๘ การกำหนดนโยบายในการให้บริการอินเตอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่อนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนด จะต้องได้รับความยินยอมจากหน่วยงานก่อน

๓.๙ การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

๓.๑๐ มีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ Firewall เป็นประจำทุกสัปดาห์หรือทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

๓.๑๑ หน่วยงานมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

๓.๑๒ ผู้ละเมิดนโยบายด้านความปลอดภัยของ Firewall จะถูกระงับการใช้งานอินเตอร์เน็ตทันที

ส่วนที่ ๑๑
แนวปฏิบัติการรับมือเหตุภัยคุกคามทางไซเบอร์

๑. วัตถุประสงค์

เพื่อใช้เป็นแนวปฏิบัติการในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใน กรมพัฒนาฝีมือแรงงาน โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่าง ๆ ภายใต้ กรมพัฒนาฝีมือแรงงาน การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสียเพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของ กรมพัฒนาฝีมือแรงงาน

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบเครือข่าย

๒.๓ ผู้ดูแลเครื่องแม่ข่าย

๓. แนวปฏิบัติการรับมือเหตุภัยคุกคามทางไซเบอร์ แนวปฏิบัตินี้เป็นไปตามหลักการของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อให้หน่วยงานมีแนวทางที่ชัดเจนในการรับมือกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ ตั้งแต่การป้องกันไปจนถึงการฟื้นฟูและการเรียนรู้จากเหตุการณ์ที่เกิดขึ้น

๓.๑ การเตรียมความพร้อมก่อนเกิดเหตุ เพื่อลดความเสี่ยงและเพิ่มศักยภาพในการรับมือกับภัยคุกคามทางไซเบอร์ หน่วยงานควรมีการเตรียมความพร้อมดังนี้:

๑) จัดทำประมวลแนวทางปฏิบัติ กรอบมาตรฐาน และแผนรับมือภัยคุกคามทางไซเบอร์ที่สอดคล้องกับบริบทของหน่วยงาน

๒) จัดตั้งทีมรับมือภัยคุกคามไซเบอร์ (CSIRT) หรือทีมที่มีบทบาทเทียบเท่า เพื่อเป็นศูนย์กลางในการประสานงานและดำเนินการเมื่อเกิดเหตุ

๓) จัดให้มีระบบการเฝ้าระวัง แจ้งเตือน และบันทึกข้อมูลจราจรคอมพิวเตอร์ (Log) ที่เป็นไปตามมาตรฐาน เพื่อตรวจจับความผิดปกติได้ทันท่วงที

๓.๒ ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคาม (Detection and Analysis) เมื่อเกิดเหตุการณ์ที่อาจเป็นภัยคุกคามไซเบอร์ หน่วยงานต้องดำเนินการตรวจจับและวิเคราะห์อย่างรวดเร็วและแม่นยำ โดยมีกระบวนการ ดังนี้

๑) จัดให้มีกลไกเพื่อตรวจจับสัญญาณของภัยคุกคามทางไซเบอร์จากทั้งแหล่งข้อมูลภายในและภายนอก เช่น การแจ้งเตือนจาก ThaiCERT

๒) รับและประมวลผลการแจ้งเตือนภัยที่มาจากระบบต่าง ๆ เพื่อระบุภัยคุกคามที่อาจเกิดขึ้น

๓) จัดเก็บและวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ (Log) และข้อมูลที่เกี่ยวข้องจากอุปกรณ์และระบบรักษาความปลอดภัยต่าง ๆ เช่น IDS, Firewall, Antivirus Logs

๔) ศึกษาและเปรียบเทียบพฤติกรรมการทำงานของระบบในช่วงเวลาที่เกิดเหตุกับพฤติกรรมปกติ (Baseline) เพื่อระบุความผิดปกติ

๕) ดำเนินการสืบค้นและรวบรวมข้อมูลทั้งหมดที่เกี่ยวข้องกับเหตุการณ์ เช่น ประเภทของภัยคุกคาม ช่องโหว่ที่ถูกโจมตี ขอบเขตของผลกระทบ (เช่น ระบบที่ได้รับผลกระทบ ผู้ใช้งาน เวลา Payload หรือข้อมูล Log) และสถานการณ์การโจมตี (เช่น กำลังเกิดขึ้น หรือสิ้นสุดแล้ว)

๖) จำแนกภัยคุกคามตามประเภท เช่น DDoS, Malware, Phishing เพื่อให้ง่ายต่อการวางแผนรับมือ

๗) ประเมินผลกระทบที่อาจเกิดขึ้นและจัดลำดับความสำคัญของเหตุการณ์ตามระดับความรุนแรง เพื่อให้สามารถจัดสรรทรัพยากรได้อย่างเหมาะสม

๘) แจ้งหน่วยงานหรือบุคลากรที่รับผิดชอบตามช่องทางที่ปลอดภัยและคำนึงถึงระดับชั้นความลับของข้อมูล

๙) รายงานเหตุการณ์สำคัญต่อหน่วยงานกำกับดูแลภายในระยะเวลาที่กำหนด เพื่อให้มีการประสานงานและรับมือในภาพรวม

๓.๓ ขั้นการระงับภัยคุกคาม การปราบปราม และการฟื้นฟูระบบ (Containment, Eradication, Recovery) หลังจากตรวจพบและวิเคราะห์ภัยคุกคามแล้ว หน่วยงานต้องดำเนินการระงับ ยับยั้ง และฟื้นฟูระบบให้กลับมาทำงานได้ตามปกติ โดยมีกระบวนการ ดังนี้

๑) ในกรณีเร่งด่วน ให้ดำเนินการปิดระบบหรือตัดการเชื่อมต่อจากเครือข่ายชั่วคราว เพื่อควบคุมและจำกัดความเสียหายไม่ให้ลุกลาม

๒) ดำเนินการแก้ไขปัญหาในเบื้องต้น เช่น ปิดบัญชีผู้ใช้ที่ถูกละเมิด ลบมัลแวร์ หรือหยุดบริการที่ถูกเจาะระบบ

๓) หากไม่สามารถแก้ไขปัญหาด้วยตนเองได้ จะแจ้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อขอคำแนะนำหรือความช่วยเหลือจากผู้เชี่ยวชาญ

๔) จัดเก็บพยานหลักฐานทางดิจิทัลที่เกี่ยวข้องอย่างเป็นระบบ เพื่อใช้สำหรับการวิเคราะห์ทางนิติวิทยาศาสตร์และเป็นหลักฐานในการดำเนินคดี

๕) ดำเนินการตรวจหาต้นตอของการโจมตี เช่น IP Address, ช่องโหว่ที่ถูกใช้, หรือเส้นทางการโจมตี เพื่อทำความเข้าใจวิธีการโจมตี

๖) ดำเนินการจัดการกับช่องโหว่ที่ถูกใช้ในการโจมตี เช่น ปรับแต่ง Firewall, ติดตั้ง Patch ระบบ, หรืออัปเดตโปรแกรม Antivirus

๗) ดำเนินการฟื้นฟูระบบให้กลับมาทำงานได้ตามปกติ ซึ่งอาจรวมถึง:

- กู้คืนระบบจากข้อมูลสำรอง (Backup)
- เปิดใช้งานระบบสำรอง (ถ้ามี)
- ติดตั้งระบบใหม่ในกรณีที่เสียหายรุนแรง
- เปลี่ยนรหัสผ่านของผู้ใช้งานและระบบ
- ตรวจสอบความพร้อมและประสิทธิภาพของระบบอย่างละเอียดก่อนเปิดใช้งานอีกครั้ง

๓.๔ ขั้นตอนหลังเหตุการณ์ (Post-Incident Activities) หลังจากจัดการกับภัยคุกคามและฟื้นฟูระบบแล้ว ดำเนินการทบทวนและปรับปรุงกระบวนการเพื่อป้องกันเหตุการณ์ในอนาคต โดยมีกระบวนการ ดังนี้

๑) วิเคราะห์เหตุการณ์ย้อนหลังอย่างละเอียด เพื่อระบุสาเหตุที่แท้จริง จุดอ่อนของระบบและกระบวนการ และปัจจัยอื่น ๆ ที่เกี่ยวข้อง

๒) รายงานสรุปเหตุการณ์ที่เกิดขึ้น พร้อมข้อเสนอแนะในการปรับปรุงมาตรการและแนวทางปฏิบัติ

๓) นำผลการวิเคราะห์มาปรับปรุงนโยบาย มาตรการ แนวปฏิบัติ และแผนรับมือภัยคุกคามทางไซเบอร์ให้มีความทันสมัยและมีประสิทธิภาพมากยิ่งขึ้น

๔) จัดฝึกอบรมหรือซ้อมแผนรับมือภัยคุกคามไซเบอร์สำหรับบุคลากรอย่างสม่ำเสมอ เพื่อให้พร้อมเมื่อเกิดเหตุการณ์จริง

๕) จัดเก็บหลักฐานดิจิทัลตามระยะเวลาที่กำหนด เพื่อใช้ในการดำเนินคดีหรือตรวจสอบย้อนหลังหากมีความจำเป็น

๖) หากการโจมตีเข้าข่ายความผิดทางอาญา หรือตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ให้พิจารณาร้องทุกข์ตามกฎหมายต่อไป

นโยบายการสำรองข้อมูลและการเตรียมความพร้อมกรณีฉุกเฉิน

๑. วัตถุประสงค์

๑.๑ เพื่อให้ระบบสารสนเทศของหน่วยงาน ให้บริการได้อย่างต่อเนื่อง

๑.๒ เพื่อเป็นมาตรฐาน แนวทางปฏิบัติ และความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานเป็นไปอย่างเคร่งครัด โดยสามารถดำเนินการสำรองข้อมูล ได้อย่างถูกต้อง และมีการเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่จำเป็น

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลเครื่องแม่ข่าย

๓. แนวปฏิบัติ

๓.๑ การคัดเลือกการสำรองข้อมูล

มีการพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานตามแนวทางต่อไปนี้

๓.๑.๑ ต้องสำรองข้อมูลสำคัญ รวมถึงโปรแกรมระบบปฏิบัติการ โปรแกรมระบบงานคอมพิวเตอร์ และชุดคำสั่งที่ใช้ทำงานให้ครบถ้วน ให้สามารถพร้อมใช้งานได้อย่างต่อเนื่อง

๓.๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

๑) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่นการสำรองข้อมูลแบบเต็ม (full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๔) ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ได้แก่ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลตั้งค่า (Configuration) ข้อมูลในฐานข้อมูล

๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้น

๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น

๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๙) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๑๐) ตรวจสอบและทดสอบประสิทธิภาพ และประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๑๑) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๓.๒ จัดทำแผนเตรียมความพร้อมฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจตามแนวทางต่อไปนี้

๓.๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้นและกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๖) การสร้างความตระหนัก หรือให้ความรู้ แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๓.๒.๒ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๓.๒.๓ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๔ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๕ มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๓.๓ การสำรองข้อมูลและกู้คืนข้อมูล

๓.๓.๑ วิเคราะห์และประเมินความสำคัญระบบสารสนเทศที่จำเป็นต้องมีการสำรองข้อมูลกำหนดผู้รับผิดชอบในการสำรองข้อมูล

๓.๓.๒ การสำรองข้อมูล ต้องประกอบด้วยการสำรองประเภทของข้อมูลอย่างน้อยดังต่อไปนี้

๑) ข้อมูลตั้งค่า (Configuration) สำหรับระบบ

๒) ข้อมูลคู่มือการปฏิบัติงานสำหรับระบบ

๓) ข้อมูลในฐานของระบบงาน (กรณีที่เป็นระบบงาน)

๔) ข้อมูลในฐานข้อมูล เช่น ซอฟต์แวร์ระบบงาน และซอฟต์แวร์ระบบงาน และซอฟต์แวร์อื่น ๆ เป็นต้น

๓.๓.๓ ผู้ดูแลเครื่องแม่ข่ายต้องตั้งค่าระบบให้สำรองข้อมูลโดยอัตโนมัติ หรือทำการสำรองข้อมูลของระบบซึ่งอยู่ในความรับผิดชอบของตนเองตามความเหมาะสมของแต่ละระบบ ไม่ต่ำกว่า ๑ ครั้งต่อเดือน

๓.๓.๔ ผู้ดูแลเครื่องแม่ข่ายต้องตั้งค่าสำรองข้อมูลอัตโนมัติสำหรับเครื่องคอมพิวเตอร์แม่ข่ายของ เว็บไซต์ (Web Server)

๓.๓.๕ เครื่องคอมพิวเตอร์ทั่วไป จะต้องทำการสำรองข้อมูลในเครื่องคอมพิวเตอร์ตามความเหมาะสม ไม่ต่ำกว่า ๑ ครั้งต่อเดือน

๓.๓.๖ เมื่อองค์กรประกาศให้มีการสำรองข้อมูลเนื่องจากจะได้มีการดำเนินการที่อาจส่งผลต่อข้อมูลในเครื่องคอมพิวเตอร์ผู้ใช้ ผู้ใช้จะต้องทำการสำรองข้อมูลดังกล่าวภายในระยะเวลาที่กำหนด

๓.๓.๗ หากผู้ดูแลระบบหรือเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใดเป็นข้อมูลสำคัญให้พิมพ์ (Print) ออกมาเก็บสำรองไว้ในรูปของเอกสารกระดาษ (Hard Copy)

๓.๓.๘ ผู้ดูแลเครื่องแม่ข่ายต้องทำการทดสอบกู้ข้อมูลสำรองในทุกระบบ โดยต้องมีการทดสอบอย่างน้อยปีละ ๑ ครั้ง ซึ่งการทดสอบดังกล่าว ต้องใช้ข้อมูลสำรองจากระบบที่ใช้งานจริง แต่ทดสอบบนระบบทดสอบ

๓.๓.๙ ผู้ดูแลเครื่องแม่ข่ายต้องทำการสำรองข้อมูลอิเล็กทรอนิกส์ขององค์กร และเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูลขององค์กร โดยต้องมีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลที่สำคัญ

๓.๓.๑๐ ต้องเปิดใช้งานการกู้คืน (Recovery) ของระบบปฏิบัติการตลอดเวลา

๓.๓.๑๑ ผู้ดูแลเครื่องแม่ข่ายต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟต์แวร์ใหม่เพื่อทดแทนของเดิมที่เสียหาย

๓.๓.๑๒ ผู้ดูแลเครื่องแม่ข่ายต้องทำการบำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์สนับสนุนเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

๓.๓.๑๓ ต้องเปิดใช้งานการกู้คืน (Recovery) ของระบบปฏิบัติการตลอดเวลา

๓.๓.๑๔ ผู้ดูแลเครื่องแม่ข่ายต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟต์แวร์ใหม่เพื่อทดแทนของเดิมที่เสียหาย

๓.๓.๑๕ ผู้ดูแลเครื่องแม่ข่ายต้องทำการบำรุงรักษาระบบคอมพิวเตอร์ และอุปกรณ์สนับสนุนเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

๓.๔ กำหนดความถี่ในการสำรองข้อมูลและกู้คืนข้อมูล ดังนี้

๓.๔.๑ สำรองข้อมูลตามความถี่ที่กำหนดไว้ ตรวจสอบว่าการสำรองที่เกิดขึ้นนั้นสำเร็จครบถ้วนหรือไม่ หากไม่สำเร็จให้หาสาเหตุดำเนินการแก้ไข และดำเนินการใหม่อีกครั้งหนึ่ง

๓.๔.๒ นำข้อมูลที่สำรองได้นั้นเก็บไว้ทั้งใน และนอกสถานที่อย่างน้อยอย่างละ ๑ ชุด

๓.๔.๓ ทดสอบกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ (ปีละ ๑ ครั้ง) เพื่อดูว่าข้อมูล ยังสามารถใช้งานได้ตามปกติหรือไม่

๓.๔.๔ จัดทำหรือปรับปรุงขั้นตอนปฏิบัติในการสำรอง และกู้คืนข้อมูล โดยให้มีการปฏิบัติตามแนวทางปฏิบัติสำหรับการสำรอง และทดสอบกู้คืนข้อมูล

นโยบายการบริหารจัดการการเข้าถึงข้อมูล

๑. วัตถุประสงค์

๑.๑ เพื่อให้ข้อมูลที่จัดเก็บในองค์กรมีความมั่นคงปลอดภัยและป้องกันความเสี่ยงจากภัยคุกคาม

๑.๒ เพื่อเป็นมาตรฐาน แนวทางปฏิบัติ และความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานเป็นไปอย่างเคร่งครัด โดยสามารถดำเนินการบริหารจัดการหรือประมวลผลข้อมูลในองค์กร ได้อย่างถูกต้อง

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบสารสนเทศ

๒.๓ ผู้ดูแลระบบเครือข่าย

๒.๔ ผู้ดูแลเครื่องแม่ข่าย

๓. แนวปฏิบัติ

๓.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ โดยแบ่งชั้นความลับของข้อมูล เป็น ๓ ระดับ ดังนี้

๓.๑.๑ ลับที่สุด หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งภาครัฐร้ายแรงที่สุด

๓.๑.๒ ลับมาก หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วน จะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

๓.๑.๓ ลับ หมายถึง ข้อมูลลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

๓.๒ เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๓.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล หรือใช้การพิสูจน์ตัวตนด้วย Token Key

๓.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น

๓.๕ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๓.๖ ผู้ดูแลระบบ ต้องกำหนดวิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๓.๗ การบริหารจัดการกับข้อมูล ต้องมีการตรวจสอบความถูกต้องเหมาะสมของข้อมูลที่จะเผยแพร่ออกสู่สาธารณะผ่านทางเว็บไซต์ ข้อมูลดังกล่าวจะต้องไม่ขัดต่อกฎหมายและมีกลไกป้องกันการเข้าไปแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(IT Risk Management)

๑. วัตถุประสงค์

๑.๑ เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๑.๒ เพื่อเป็นการป้องกัน และลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

๒. ผู้รับผิดชอบ

๒.๑ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒.๒ ผู้ดูแลระบบเครือข่าย

๓. แนวปฏิบัติ

๓.๑ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๓.๑.๑ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๓.๑.๒ มีการตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบระบบสารสนเทศภายในของหน่วยงาน (Internal IT Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศ

๓.๒ แนวทางการตรวจสอบและประเมินความเสี่ยง ดังนี้

๓.๒.๑ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๒ มีการทบทวนนโยบาย และมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๓.๒.๓ มีการตรวจสอบและประเมินความเสี่ยง และให้จัดทำรายงานพร้อมข้อเสนอแนะ

๓.๒.๔ มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๓) กำหนดให้มีการระบุ และจัดสรรทรัพยากรที่จำเป็นต้องใช้ ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวัน และเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริง หรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศฉบับนี้ ได้ผ่านการพิจารณาจากผู้บริหารเทคโนโลยีสารสนเทศระดับกรม ของกรมพัฒนาฝีมือแรงงานเพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการเพื่อจัดการความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศต่อไป

(นายภัทรวุธ เภอแสละ)
ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม

ภาคผนวก

ภาคผนวก ก.
การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน

วิธีการบริหารจัดการรหัสผ่านของเจ้าหน้าที่ให้มีความมั่นคงปลอดภัย

เพื่อให้การตั้งรหัสผ่าน (Password) สำหรับการเข้าใช้งานระบบสารสนเทศของกรมพัฒนาฝีมือแรงงานเป็นไปอย่างมั่นคงปลอดภัย และลดความเสี่ยงจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ขอให้ผู้ใช้งานถือปฏิบัติตามแนวทางดังต่อไปนี้:

๑. คุณลักษณะของรหัสผ่านที่เหมาะสม ต้องมีความยาว อย่างน้อย ๘ ตัวอักษร

๒. ต้องประกอบด้วยอักขระจากอย่างน้อย ๓ ใน ๔ กลุ่มต่อไปนี้

- ตัวอักษรภาษาอังกฤษ พิมพ์ใหญ่ (A–Z)
- ตัวอักษรภาษาอังกฤษ พิมพ์เล็ก (a–z)
- ตัวเลข (๐–๙)
- อักขระพิเศษ (! @ # $ % ^ & * ( ) _ - + =)

๓. ห้ามใช้รหัสผ่านที่คาดเดาได้ง่าย เช่น “๑๒๓๔๕๖๗๘”, “password”, “admin”, วันเดือนปีเกิด หรือชื่อของผู้ใช้งาน

๔. ห้ามใช้รหัสผ่านเดิมซ้ำ เมื่อทำการเปลี่ยนรหัสผ่าน

๕. ไม่ควรใช้รหัสผ่านเดียวกันกับระบบอื่น เช่น อีเมลส่วนตัว เฟซบุ๊ก ฯลฯ)

๖. แนวปฏิบัติในการรักษาความปลอดภัยของรหัสผ่าน

- ห้ามเปิดเผยรหัสผ่านของตนเองแก่ผู้อื่นไม่ว่าในกรณีใด ๆ
- ห้ามเขียนหรือบันทึกรหัสผ่านไว้ในที่ที่ผู้อื่นสามารถเข้าถึงได้
- หากสงสัยว่ารหัสผ่านอาจถูกเปิดเผยหรือรั่วไหล ต้องเปลี่ยนรหัสผ่านทันที
- ควรเปลี่ยนรหัสผ่านอย่างน้อย ทุก ๖ เดือน

ทะเบียนผู้มีสิทธิ์เข้าออก ห้องคอมพิวเตอร์แม่ข่าย

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ลำดับที่	ชื่อ-นามสกุล	ตำแหน่ง
๑	นายชาตรี กอบัวแก้ว	ผู้เชี่ยวชาญด้านเทคโนโลยีและสารสนเทศ
๒	นายปพน โสตถิโภคา	นักวิชาการคอมพิวเตอร์ชำนาญการ
๓	นายกิตติศักดิ์ แซ่หลี	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๔	นายกันต์ธพจน์ ลีรตานนท์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๕	นางสาวอณิมา ไพรสินธ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๖	นางสาวศิริพันธุ์ สุทธิเชาวนะพันธุ์	นักวิชาการคอมพิวเตอร์
๗	นายธีรัช สุเทวี	นักวิชาการคอมพิวเตอร์
๘	นายสมยศ มากชุมโค	นักวิชาการคอมพิวเตอร์
๙	นายสุริยา บุดศรี	นักวิชาการคอมพิวเตอร์
๑๐	นายปรัชญา เอี่ยมอำภา	นักวิชาการคอมพิวเตอร์
๑๑	นายณัฐพงศ์ เสียงหวาน	นักวิชาการคอมพิวเตอร์
๑๒	นายทัชชกร จันทรคุณาภาศ	นักวิชาการคอมพิวเตอร์

บันทึกการเข้าออก ห้องคอมพิวเตอร์แม่ข่าย

ชื่อ-นามสกุล	หน่วยงาน/บริษัท	ลายเซ็น	ว/ด/ป	เวลาเข้า	เวลาออก	หมายเหตุ