แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมการพัฒนาชุมชน พ.ศ. ๒๕๖๒

กรมการพัฒนาชุมชน กระทรวงมหาดไทย

แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมการพัฒนาชุมชน พ.ศ. ๒๕๖๒

กรมการพัฒนาชุมชน กระทรวงมหาดไทย

คำนำ

ปัจจุบันระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับหน่วยงาน โดยช่วยให้การติดต่อสื่อสารมีประสิทธิภาพและประหยัดต้นทุนในการดำเนินงาน อย่างไรก็ตาม แม้ระบบเทคโนโลยีสารสนเทศจะมีประโยชน์และอำนวยความสะดวกในด้านต่าง ๆ แต่ก็มีความเสี่ยงต่อการถูกโจมตีจากผู้ไม่หวังดีได้มากขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบหรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเตอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ซึ่งสิ่งเหล่านี้ เป็นการสร้างความเสียหายด้านระบบสารสนเทศเป็นอย่างมาก ทั้งยังส่งผลทางลบต่อชื่อเสียงหรือภาพพจน์ของหน่วยงาน ดังนั้น ผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการดูแลบำรุงรักษาและการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง โดยมีหลักสำคัญด้วยกัน ๓ ประการ คือ ความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) เพื่อให้เป็นไปตามมาตรฐานสากล

ดังนั้น กรมการพัฒนาชุมชน จึงได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปี ๒๕๖๒ ซึ่งดำเนินการภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และฉบับที่ ๒ พ.ศ. ๒๕๕๖ เพื่อให้หน่วยงานทั้งส่วนกลางและภูมิภาค ใช้เป็นแนวทางเสริมสร้างความมั่นคงปลอดภัยแก่ระบบสารสนเทศชุมชน

กรมการพัฒนาชุมชน จึงหวังเป็นอย่างยิ่งว่าแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบและผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของกรมการพัฒนาชุมชนทุกระดับ ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานต่อไป

กรมการพัฒนาชุมชน
มีนาคม ๒๕๖๒

สารบัญ

สารบัญ

ประกาศกรมการพัฒนาชุมชน
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมการพัฒนาชุมชน พ.ศ. ๒๕๖๒

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ อธิบดีกรมการพัฒนาชุมชน โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมการพัฒนาชุมชน เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศของกรมการพัฒนาชุมชน พ.ศ. ๒๕๖๒”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓ คำนิยาม ประกอบด้วย

(๑) “กรมการพัฒนาชุมชน” หมายความว่า หน่วยงานตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ. ๒๕๔๕

(๒) “ส่วนกลาง” หมายความว่า สำนัก/สถาบัน/กอง/ศูนย์ และรวมถึงศูนย์ศึกษาและพัฒนาชุมชนทุกแห่ง ที่สังกัดกรมการพัฒนาชุมชน

(๓) “ส่วนภูมิภาค” หมายความว่า สำนักงานพัฒนาชุมชนจังหวัดและทุกหน่วยงานที่สังกัดกรมการพัฒนาชุมชน

(๔) “ศูนย์สารสนเทศเพื่อการพัฒนาชุมชน” หมายความว่า หน่วยงานตามกฎกระทรวงแบ่งส่วนราชการกรมการพัฒนาชุมชน กระทรวงมหาดไทย พ.ศ. ๒๕๕๒

(๕) “ผู้บริหาร” หมายความว่า อธิบดีกรมการพัฒนาชุมชนหรือผู้ที่อธิบดีกรมการพัฒนาชุมชนมอบหมาย

(๖) “ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)” หมายความว่า ผู้ที่มีชื่อในคำสั่งแต่งตั้ง มีหน้าที่

๑) กำหนดนโยบายด้านการควบคุม การใช้ระบบคอมพิวเตอร์และเครือข่าย

๒) ให้คำปรึกษาแก่ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

๓) รายงานเหตุการณ์และผลการปฏิบัติงานตามระเบียบให้ อธิบดีกรมการพัฒนาชุมชนทราบ

(๗) “ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์” (System Administrator) หมายความว่า ผู้ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลรักษาเครือข่ายคอมพิวเตอร์และสามารถเข้าถึงโปรแกรม รวมทั้งอุปกรณ์เครือข่ายคอมพิวเตอร์เพื่อการบริหารจัดการ แบ่งเป็น ๒ ส่วน

ส่วนกลาง

ก. ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

๑) เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการใช้ระบบคอมพิวเตอร์และเครือข่ายระดับกรมการพัฒนาชุมชน

๒) มีอำนาจสั่งการให้หยุดหรือปฏิบัติการระงับเหตุที่เกิดขึ้นจากการไม่ปฏิบัติตามประกาศนี้

๓) รายงานเหตุการณ์และผลการปฏิบัติงานตามประกาศให้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบ

ข. ผู้อำนวยการกลุ่มงานพัฒนาระบบเครือข่าย

๑) เป็นผู้วิเคราะห์สถานการณ์และแจ้งเหตุการณ์ต่อผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน เพื่อระงับเหตุการณ์จากการไม่ปฏิบัติตามประกาศของผู้ใช้งานต่อผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

๒) มีอำนาจสั่งการแทนผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน ในกรณีที่ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนไม่สามารถปฏิบัติราชการได้

ส่วนภูมิภาค

ก. พัฒนาการจังหวัดทุกจังหวัด

๑) เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการใช้ระบบคอมพิวเตอร์และเครือข่ายระดับจังหวัด

๒) มีอำนาจสั่งการให้หยุด หรือปฏิบัติการระงับเหตุที่เกิดขึ้นจากการไม่ปฏิบัติตามประกาศนี้

๓) รายงานเหตุการณ์และผลการปฏิบัติงานตามระเบียบให้ ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนทราบ

ข. หัวหน้ากลุ่มงานสารสนเทศการพัฒนาชุมชน สำนักงานพัฒนาชุมชนจังหวัด

๑) เป็นผู้วิเคราะห์สถานการณ์ในระดับสำนักงานพัฒนาชุมชนจังหวัด สำนักงานพัฒนาชุมชนอำเภอและแจ้งเหตุการณ์ต่อพัฒนาการจังหวัด เพื่อระงับเหตุการณ์ไม่ปฏิบัติตามประกาศของผู้ใช้งานต่อพัฒนาการจังหวัด

๒) มีอำนาจสั่งการแทนพัฒนาการจังหวัด ในกรณีที่พัฒนาการจังหวัดไม่สามารถปฏิบัติราชการได้

(๘) “ผู้ใช้งาน (User)” หมายความว่า ข้าราชการสังกัดกรมการพัฒนาชุมชนรวมถึงลูกจ้างและพนักงานราชการหรือบุคคลภายนอกที่ได้รับมอบหมายให้ปฏิบัติงาน ตามสัญญาของกรมการพัฒนาชุมชน

(๙) “สิทธิของผู้ใช้งาน (User Management)” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน และกำหนดระดับสิทธิในการเข้าถึงระบบด้วยการกำหนดบัญชีผู้ใช้งาน

(๑๐) “บัญชีผู้ใช้งาน (User Account)” หมายความว่า บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งานระบบคอมพิวเตอร์ ซึ่งเป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบคอมพิวเตอร์

(๑๑) “ชื่อผู้ใช้ (Username)” หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

(๑๒) “รหัสผ่าน (Password)” หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(๑๓) “เครือข่ายคอมพิวเตอร์” หมายความว่า เครือข่ายคอมพิวเตอร์ของกรมการพัฒนาชุมชน

(๑๔) “เครื่องคอมพิวเตอร์” หมายความว่า อุปกรณ์ประมวลผลข้อมูลที่ทำงานด้วยระบบอิเล็กทรอนิกส์ที่มีความเร็วสูง โดยทำงานตามคำสั่งผ่านทางซอฟต์แวร์ให้ได้ผลตามที่ต้องการ ซึ่งได้แก่ คอมพิวเตอร์แม่ข่าย (Server) คอมพิวเตอร์ส่วนบุคคล (Personal Computer) และคอมพิวเตอร์แบบพกพา (Notebook Computer)

(๑๕) “อุปกรณ์คอมพิวเตอร์” หมายความว่า อุปกรณ์อิเล็กทรอนิกส์ที่ใช้งานร่วมกับเครื่องคอมพิวเตอร์เพื่อสนับสนุนให้เครื่องคอมพิวเตอร์ปฏิบัติงานได้ตามต้องการ

(๑๖) “สินทรัพย์” หมายความว่า สิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับหน่วยงาน

(๑๗) “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาตการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๑๘) “ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่นได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

(๑๙) “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๒๐) “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

(๒๑) “ระบบอินเทอร์เน็ต (Internet)” หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตสากล

(๒๒) “ระบบสารสนเทศ” หมายความว่า ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

(๒๓) “หน่วยงานภายนอก” หมายความว่า องค์กรหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจ หน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

(๒๔) “ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะจัดทำในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

(๒๕) “การเข้ารหัส (Encryption)” หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

(๒๖) “จดหมายอิเล็กทรอนิกส์ (E-mail)” หมายความว่า ระบบที่บุคคลใช้ในการรับ - ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับ - ส่งข้อมูลชนิดนี้ ได้แก่ SMTP , POP๓ และ IMAP เป็นต้น

(๒๗) “สื่อบันทึกพกพา” หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือThumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

(๒๘) “อุปกรณ์จัดเส้นทาง (Router)” หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

(๒๙) “การพิสูจน์ยืนยันตัวตน (Authentication)” หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไป โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

(๓๐) “SSID (Service Set Identifier)” หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

(๓๑) “WEP (Wired Equivalent Privacy)” หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้น ทุกเครื่องในเครือข่ายที่รับ - ส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

(๓๒) “WPA (Wi-Fi Protected Access)” หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

(๓๓) “MAC Address (Media Access Control Address)” หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอินเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหลายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่รูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

(๓๔) “VPN (Virtual Private Network)” หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับ - ส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ - ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

(๓๕) “แผนผังระบบเครือข่าย (Network Diagram)” หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

ข้อ ๔ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ ตามประกาศนี้ มี ๒ ส่วนดังนี้

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๕

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๖ - ๑๔

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วนดังนี้

(๑) ส่วนที่ว่าด้วยการจัดทำนโยบาย

๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของกรมการพัฒนาชุมชน

๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๔) ให้ทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

(๒) ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีนโยบายในการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรมและเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๖ ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) อย่างน้อย ดังนี้

(๑) ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจของหน่วยงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง

ข้อ ๗ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้วและผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยของสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตอย่างน้อย ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๘ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๙ การควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตอย่างน้อย ดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งานและกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

(๘) การควบคุมการเข้าใช้งานระบบจากภายนอก

(๙) การใช้งานระบบเครือข่ายอินเทอร์เน็ต (Internet)

ข้อ ๑๐ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาตอย่างน้อย ดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) จำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุมอย่างน้อย ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๒ จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองและการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้

(๑) ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๔ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) และผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ ทบทวนให้เป็นปัจจุบันอยู่เสมอ ให้ใช้แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่แนบท้ายประกาศนี้

ข้อ ๑๕ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติ ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้อธิบดีกรมการพัฒนาชุมชน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ ๕ มีนาคม พ.ศ. ๒๕๖๒

(นายนิสิต จันทร์สมวงศ์)
อธิบดีกรมการพัฒนาชุมชน

เอกสารแนบท้ายประกาศ
เรื่อง แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของกรมการพัฒนาชุมชน พ.ศ. ๒๕๖๒

ส่วนที่ ๑

นโยบายควบคุมการเข้าถึง และการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงานรับรู้ เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) กรมการพัฒนาชุมชน
๒. ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน กรมการพัฒนาชุมชน
๓. ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control)

๑.๑ จัดทำบัญชีสินทรัพย์หรือทะเบียนสินทรัพย์ การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

(๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทข้อมูล

- ข้อมูลสารสนเทศด้านบริหาร เช่น ข้อมูลบุคลากร ข้อมูลงบประมาณ การเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศเพื่อการพัฒนาชุมชน เช่น ข้อมูลหมู่บ้านเศรษฐกิจพอเพียง ข้อมูลผู้นำชุมชน ข้อมูลสินค้า OTOP ข้อมูล จปฐ. กชช.๒ค เป็นต้น

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร สามารถเข้าถึงข้อมูลทุกลำดับชั้นความลับของข้อมูล
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป สามารถเข้าถึงลำดับชั้นข้อมูลทั่วไป เท่านั้น
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย สามารถเข้าถึงลำดับชั้นข้อมูลทั่วไป โดยข้อมูลลับที่สุด ข้อมูลลับมากและข้อมูลลับ ต้องได้รับอนุญาตจากผู้บริหารเป็นลายลักษณ์อักษร

(๕) การกำหนดเวลาที่ได้เข้าถึง ดังนี้

- ข้อมูลสารสนเทศด้านบริหารให้เป็นไปตามห้วงเวลาที่หน่วยงานประกาศ
- ข้อมูลสารสนเทศเพื่อการพัฒนาชุมชนสามารถเข้าถึงได้ ๒๔ ชั่วโมง

(๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

๑.๔ ผู้ดูแลระบบ ต้องจัดให้ใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑) ควบคุมการเข้าถึงสารสนเทศ โดยกำหนดการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(๒) ปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๒.๑ เพื่อรักษาความปลอดภัยแก่เครื่องคอมพิวเตอร์ได้เหมาะสมตามระดับความเสี่ยง ให้ศูนย์สารสนเทศเพื่อการพัฒนาชุมชนกำหนดวิธีประเมินความเสี่ยงเพื่อใช้เป็นมาตรฐานในการจัดประเภทคอมพิวเตอร์ตามลำดับความเสี่ยง โดยแบ่งออกเป็น ๓ ระดับ คือ

(๑) เครื่องคอมพิวเตอร์ที่อยู่ในระดับความเสี่ยงสูง

(๒) เครื่องคอมพิวเตอร์ที่อยู่ในระดับความเสี่ยงปานกลาง

(๓) เครื่องคอมพิวเตอร์ที่อยู่ในระดับความเสี่ยงต่ำ

๒.๒ การรักษาความปลอดภัยแก่เครื่องคอมพิวเตอร์ทางกายภาพ ให้พิจารณาสถานที่ติดตั้งและเก็บรักษาเครื่องคอมพิวเตอร์ของกรมการพัฒนาชุมชน ๔ ระดับ คือ

(๑) เขตหวงห้ามเด็ดขาด (Exclusion Area) คอมพิวเตอร์แม่ข่ายต้องจัดพื้นที่ให้เป็นเขตหวงห้ามเด็ดขาด ต้องตั้งอยู่ในบริเวณด้านในที่มีการสัญจรไปมาน้อยและมีการออกแบบสถานที่เพื่อให้อุปกรณ์คอมพิวเตอร์ตั้งอยู่ภายในพื้นที่มีความปลอดภัยจากภัยคุกคามที่อาจเกิดขึ้น

(๒) เขตหวงห้ามเฉพาะ (Limited Area) ข้อมูลสำคัญจำเป็นต้องปกปิดเป็นความลับ เช่น ข้อมูลบุคลากรต้องตั้งอยู่ในบริเวณด้านในของหน่วยงานราชการและต้องมีการออกแบบสถานที่ให้อุปกรณ์คอมพิวเตอร์ตั้งอยู่ภายในพื้นที่มีความปลอดภัยจากภัยคุกคามที่อาจเกิดขึ้นเขตในความควบคุม

(๓) เขตในความควบคุมของหน่วยงานราชการ (Control Area) ต้องตั้งอยู่ในบริเวณของหน่วยงานราชการและต้องมีการออกแบบสถานที่ให้อุปกรณ์คอมพิวเตอร์ตั้งอยู่ภายในพื้นที่มีความปลอดภัยจากภัยคุกคามที่อาจเกิดขึ้น

(๔) เขตผู้มาติดต่อ (Public Area) ต้องตั้งอยู่ในบริเวณที่เข้าถึงได้สะดวก โดยต้องไม่ผ่านเขตในความควบคุมและอยู่ห่างจากเขตหวงห้ามเด็ดขาดและเขตหวงห้ามเฉพาะ ทั้งนี้ต้องมีการออกแบบสถานที่ให้อุปกรณ์คอมพิวเตอร์ตั้งอยู่ภายในพื้นที่มีความปลอดภัยจากภัยคุกคามที่อาจเกิดขึ้น

๒.๓ เพื่อประโยชน์ในการรักษาความปลอดภัยแก่สถานที่ที่ติดตั้งและเก็บรักษาเครื่องคอมพิวเตอร์ ให้ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนดำเนินการ ดังต่อไปนี้

(๑) ประสานงานกับผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ ทั้งในส่วนกลางและส่วนภูมิภาค เพื่อกำหนดแผนปฏิบัติเกี่ยวกับอัคคีภัยและเหตุฉุกเฉินต่าง ๆ และทดสอบระบบรักษาความปลอดภัย ภายในเขตรักษาความปลอดภัยอย่างน้อยปีละ ๑ ครั้ง

(๒) จัดอบรมและซักซ้อมผู้จัดการฐานข้อมูลที่ปฏิบัติงานภายในเขตรักษาความปลอดภัย ตามระยะเวลาอันสมควร เพื่อให้สามารถใช้งานอุปกรณ์รักษาความปลอดภัยได้อย่างถูกต้องและเหมาะสม

๒.๔ ให้กองคลังรับผิดชอบการบำรุงรักษาสถานที่ อุปกรณ์ป้องกันความเสียหาย และอุปกรณ์ป้องกันภัยต่าง ๆ ภายในเขตรักษาความปลอดภัย ตามระยะเวลาอันสมควรภายใต้คำแนะนำจากศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

๒.๕ เพื่อประโยชน์ในการรักษาความปลอดภัยแก่เครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ ให้ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ส่วนกลางและส่วนภูมิภาค ดำเนินการดังต่อไปนี้

(๑) กำหนดวิธีปฏิบัติในการติดตั้งและเก็บรักษาให้เหมาะสมตามระดับความเสี่ยงเพื่อป้องกันการลักลอบใช้อุปกรณ์

(๒) จัดทำทะเบียนคุมอุปกรณ์คอมพิวเตอร์ โดยมีรายละเอียดเกี่ยวกับอุปกรณ์คอมพิวเตอร์ การบำรุงรักษา และการขนย้าย

(๓) กำหนดวิธีปฏิบัติในการขนย้ายอุปกรณ์คอมพิวเตอร์ออกจากพื้นที่ติดตั้งให้เหมาะสม ตามระดับความเสี่ยง เพื่อป้องกันเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์และข้อมูลเสียหายจากการขนย้าย

(๔) รับผิดชอบการแก้ไขซ่อมแซมเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์

๒.๖ ให้หน่วยงานราชการส่วนกลางและส่วนภูมิภาค เจ้าของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ดำเนินการดังต่อไปนี้

(๑) เก็บรักษาอย่างเป็นระเบียบในสถานที่ปลอดภัยให้เหมาะสมตามระดับความเสี่ยง เพื่อป้องกันการลักลอบใช้อุปกรณ์คอมพิวเตอร์

(๒) ประสานงานกับศูนย์สารสนเทศเพื่อการพัฒนาชุมชน ในการจัดเตรียมแผนรองรับ หากอุปกรณ์คอมพิวเตอร์ได้รับความเสียหายและทดสอบแผนรองรับตามระยะเวลาอันสมควร

(๓) มอบหมายให้ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ดูแลการบำรุงรักษาอุปกรณ์คอมพิวเตอร์ และควบคุมการขนย้ายอุปกรณ์คอมพิวเตอร์ เพื่อป้องกันข้อมูลที่จัดเก็บในอุปกรณ์คอมพิวเตอร์รั่วไหล หรือถูกแก้ไข

๒.๗ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security)

(๑) ในกรณีที่ต้องการเพิ่มหรือปรับปรุงสายสัญญาณและอุปกรณ์ที่เกี่ยวข้อง ให้แจ้งผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนทุกครั้ง

(๒) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๓) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณหรือการตัดสายสัญญาณ เพื่อทำให้เกิดความเสียหาย

(๔) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๕) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดพลาด

(๖) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๗) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(๘) พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ Coaxial Cable) สำหรับระบบสารสนเทศที่สำคัญ

(๙) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๒.๘ การนำสินทรัพย์ของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

(๑) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(๒) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

(๓) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๔) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๒.๙ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-Use of Equipment)

(๑) ให้ทำลายข้อมูลที่ไม่เกี่ยวข้องในอุปกรณ์ก่อนที่จะให้ผู้อื่นนำไปใช้งานต่อ

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ก่อนให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๒.๑๐ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศให้จังหวัดเก็บไว้ในสถานที่ที่มั่นคงปลอดภัยและมีมาตรการควบคุมการเข้าถึง

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

๓.๑ การลงทะเบียนบุคลากรและบุคคลที่ปฏิบัติงานให้กับหน่วยงาน ให้ผู้ดูแลระบบกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น ทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกและการเปลี่ยนแปลงการใช้งาน ดังต่อไปนี้

(๑) จัดทำแบบฟอร์มประสงค์ขอใช้ระบบงานสารสนเทศ ระบบเครือข่ายและจดหมายอิเล็กทรอนิกส์ (E-mail) เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งานและยื่นต่อผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

(๒) มีการระบุชื่อบัญชีผู้ใช้งานแยกเป็นรายบุคคลไม่ซ้ำซ้อนกัน

(๓) จำกัดการใช้บัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีชื่อเดียวกัน และอนุญาตให้ใช้งานระบบสารสนเทศเท่าที่จำเป็น

(๔) ตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมกับหน้าที่ความรับผิดชอบ ซึ่งต้องลงนามรับทราบด้วย

(๕) หลักเกณฑ์การยกเลิกสิทธิให้เข้าถึงระบบสารสนเทศ การตัดออกจากบัญชีผู้ใช้งาน และการคืนสิทธิ ให้ปฏิบัติ ดังนี้

ก. ให้ลบบัญชีผู้ใช้งานโดยไม่ชักช้าหลังจากผู้ใช้งานพ้นสภาพการเป็นข้าราชการและลูกจ้าง โดยให้หัวหน้าหน่วยงานส่วนกลางและส่วนภูมิภาค แจ้งผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนล่วงหน้าทุกครั้งที่มีผู้ใช้งานหมดสิทธิเข้าสู่ระบบคอมพิวเตอร์

ข. การยกเลิกสิทธิการใช้งานชั่วคราว และการคืนสิทธิการใช้งานให้พิจารณาเหตุการณ์/สถานการณ์ ต่อไปนี้

- ผู้ใช้งานไม่มาปฏิบัติงานติดต่อกันเกิน ๓ เดือน ได้แก่ ลาป่วย ลาศึกษาต่อ
- มีพฤติกรรมการใช้งานที่หัวหน้าหน่วยงานราชการส่วนกลางและส่วนภูมิภาคพิจารณาแล้วเห็นว่าไม่เหมาะสม
- การคืนสิทธิการใช้งานในกรณีที่ผู้ใช้งานถูกยกเลิกสิทธิ สามารถกระทำได้ต่อเมื่อได้รับแจ้งความประสงค์จากผู้ใช้งานเป็นลายลักษณ์อักษร

ค. ในการสำรองบัญชีผู้ใช้งานให้ผู้ดูแลระบบ

- สำรองไฟล์และข้อมูลแบบออฟไลน์ทุก ๓ เดือนเป็นอย่างน้อย โดยพิจารณาจากจำนวนครั้งในการเปลี่ยนแปลงข้อมูลเป็นหลัก
- สำรองทุกครั้งที่ติดตั้งระบบงานใหม่และควรสำรองข้อมูลแบบออฟไลน์ทุกครั้งที่มีการปรับปรุงแก้ไขระบบงานบนคอมพิวเตอร์แม่ข่าย
- จัดเก็บสื่อที่ใช้สำรองข้อมูลย้อนหลังอย่างน้อย ๓ รุ่น โดยให้จัดเก็บสื่อที่ใช้สำรองข้อมูลล่าสุดในตู้นิรภัยของกรมการพัฒนาชุมชนและให้จัดเก็บสื่อที่เหลือภายในเขตหวงห้ามเด็ดขาดหรือเขตหวงห้ามเฉพาะ
- ทดสอบการกู้คืนระบบโดยจำลองจากสถานการณ์จริงทุกปี

๓.๒ ผู้ดูแลระบบ กำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญให้เป็นสิทธิเฉพาะการปฏิบัติหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา รวมทั้งต้องทบทวนสิทธิ อย่างน้อยปีละ ๑ ครั้ง ได้แก่ ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต

๓.๓ ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิของผู้ใช้งาน ดังต่อไปนี้

(๑) กำหนดประเภทของสิทธิกับผู้ใช้งานระบบสารสนเทศ โดยจำแนกประเภทสิทธิตามหน้าที่ความรับผิดชอบและต้องจัดเก็บและมอบหมายสิทธิแก่ผู้ใช้งานระบบสารสนเทศ

(๒) กรณีมีความจำเป็นต้องให้สิทธิพิเศษแก่ผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นต้องได้รับความเห็นชอบจากผู้บังคับบัญชา โดยกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและต้องมีการกำหนดสิทธิพิเศษที่ได้รับว่า ได้เข้าถึงระดับใดบ้าง และต้องกำหนดให้เป็นรหัสพิเศษที่แตกต่างจากผู้ใช้งานทั่วไป

(๓) กำหนดสิทธิของผู้ใช้งานระบบสารสนเทศของผู้ที่เกี่ยวข้อง ได้แก่ อ่านอย่างเดียว การสร้างข้อมูล การป้อนข้อมูล การแก้ไขข้อมูลและการอนุมัติ

๓.๔ ผู้ดูแลระบบ ต้องบริหารจัดการรหัสผ่านของผู้ใช้งาน ดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่ง

(๒) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือใช้จดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องการในการส่งรหัสผ่าน

(๓) กำหนดให้ผู้ใช้งาน ตอบยืนยันการได้รับรหัสผ่านทันทีและให้ผู้ใช้งานเปลี่ยนรหัสผ่านตามวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use)

(๔) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านในระบบคอมพิวเตอร์ที่ไม่มีการป้องกันการเข้าถึง

(๕) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๖) กำหนดให้รหัสผู้ใช้งานที่มีสิทธิพิเศษให้แตกต่างจากผู้ใช้งานทั่วไป

๓.๕ ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงข้อมูลตามประเภทของข้อมูล ระดับความสำคัญของข้อมูลและลำดับชั้นความลับของข้อมูล ดังนี้

(๑) กำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อตรวจสอบสิทธิการเข้าถึง

(๒) กำหนดระยะเวลาการใช้งานไม่เกิน ๙๐ นาทีต่อครั้ง และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL VPN หรือ XML Encryption

(๔) กำหนดการเปลี่ยนรหัสผ่านทุก ๖๐ วัน

(๕) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีนำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน ต้องมีการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๓.๖ ผู้ดูแลระบบ ต้องจำกัดการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) สำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความเสี่ยงสูง ดังนี้

(๑) กำหนดให้มีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ ไม่เกิน ๙๐ นาทีต่อครั้ง

(๒) ผู้ประสงค์ใช้งานสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง ให้ยื่นความประสงค์เป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

๓.๗ ต้องจัดให้มีการเสริมสร้างความรู้ ความเข้าใจ เพื่อเสริมสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness) อย่างน้อยปีละ ๑ ครั้ง ด้วยช่องทางดังต่อไปนี้

(๑) จัดประชุมเชิงปฏิบัติการ

(๒) เว็บไซต์

(๓) เอกสาร

๔. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตอย่างน้อย ดังนี้

๔.๑ ผู้ดูแลระบบ ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) ให้ผู้ดูแลระบบกำหนดให้ระบบสารสนเทศต้องควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้เท่านั้น

(๒) ให้ผู้ดูแลระบบกำหนดการระบบสารสนเทศที่สำคัญ ต้องให้สิทธิเฉพาะการฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๔.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดให้ติดตั้งซอฟต์แวร์พื้นฐานที่จำเป็น เช่น ซอฟต์แวร์ป้องกันไวรัส ไฟร์วอลล์ ในอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล

(๒) ผู้ดูแลระบบต้องกำหนดรายละเอียดหรือข้อกำหนดสำหรับการปฏิบัติงานจากระยะไกล ดังนี้

- ชนิดของงานที่อนุญาตและไม่อนุญาตสำหรับการปฏิบัติงานจากระยะไกล
- ระบบงานหรือบริการต่าง ๆ ที่อนุญาตให้เข้าถึงได้จากระยะไกล
- ชั่วโมงหรือช่วงระยะเวลาการปฏิบัติงาน
- ชั้นความลับของข้อมูลที่อนุญาตให้เข้าถึงได้

(๓) การใช้งานต้องได้รับอนุญาตผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน เป็นลายลักษณ์อักษรและได้รับการควบคุมอย่างเหมาะสมจากผู้ดูแลระบบ เพื่อป้องกันการเปิดเผยข้อมูลและการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต

(๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตนก่อนเข้าใช้งาน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

(๕) ผู้ดูแลระบบตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ด

(๖) มีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงาน อย่างน้อย ๑ วิธี

(๗) การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต ให้ตรวจสอบผู้ใช้งานด้วย

๔.๓ ให้ผู้ดูแลระบบ ระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) โดยวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายเพื่อยืนยันการเข้าถึง ดังนี้

(๑) ผู้ดูแลระบบต้องจัดทำผังเครือข่าย เพื่อควบคุมการใช้งานอย่างเหมาะสม

(๒) ใช้ MAC address และ IP ในการระบุอุปกรณ์บนเครือข่าย

๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ผู้ดูแลระบบต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย โดยวิธีปฏิบัติการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตามข้อ ๘.๑ - ๘.๗

๔.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่าย สำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

๔.๖ ผู้ดูแลระบบควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่าง ให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

(๑) ทำการตรวจสอบการเชื่อมต่อเครือข่าย

(๒) จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

(๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ควบคุมไม่ให้เปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๔.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อควบคุมการเชื่อมต่อของคอมพิวเตอร์และการไหลเวียนของข้อมูลหรือสารสนเทศ ดังนี้

(๑) ควบคุมไม่ให้เปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

(๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๔.๘ การควบคุมการเข้าใช้งานระบบจากภายนอก

(๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) การเข้าสู่ระบบจากระยะไกล (Remote Access) ต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่านหรือวิธีการเข้ารหัส เป็นต้น

(๓) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกล ต้องได้รับอนุมัติจากผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนหรือผู้ดูแลระบบ ที่ได้รับมอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

(๔) ก่อนให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอและต้องได้รับอนุมัติจากผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนหรือผู้ดูแลระบบที่ได้รับมอบหมายอย่างเป็นทางการ

(๕) การควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

(๖) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และให้ตัดการเชื่อมต่อ Port และ Modem ทันทีที่ภาระกิจเสร็จสิ้น

๔.๙ การใช้งานระบบเครือข่ายอินเทอร์เน็ต (Internet) กำหนดให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) ต้องเป็นบุคลากรสังกัดกรมการพัฒนาชุมชน สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้ดูแลระบบเครือข่ายคอมพิวเตอร์

(๒) ต้องใช้ข้อความที่สุภาพ และถูกต้องตามธรรมเนียมปฏิบัติในการใช้เครือข่ายเท่านั้น

(๓) ต้องใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิภาพ โดยเฉพาะการดาวน์โหลดไฟล์ที่มีขนาดใหญ่ หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

(๔) ต้องรับผิดชอบต่อข้อมูลของตนเอง ไม่ว่าจะเก็บไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (Server) หรือการส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์

(๕) ต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชี ของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีต้องเป็นผู้รับผิดชอบ

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการของเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องปฏิบัติอย่างน้อย ดังนี้

๕.๑ การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๑) ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์

(๒) ต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๐ นาที ให้ทำการล็อคหน้าจอเมื่อไม่ใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน

(๓) ต้องทำการ Logout ออกจากระบบทันทีที่เลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๕.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน

(๑) การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง มีข้อปฏิบัติดังนี้

- ต้องมีชื่อผู้ใช้งาน (User name) และแสดงตัวตน (ID) ด้วยชื่อผู้ใช้ (Username)
- การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password) โดยระบบมีการจำกัดระยะเวลาในการป้อนรหัสผ่านและสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง
- สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม ได้แก่ Smart Card ร่วมได้

(๒) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบสารสนเทศเพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบสารสนเทศ ตามข้อปฏิบัติ ดังนี้

- ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลอันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

- ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับ ห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่ายหรือแจกจ่ายให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

- ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๕.๓ การบริหารจัดการรหัสผ่าน

(๑) ผู้ดูแลระบบต้องกำหนดขั้นตอนการปฏิบัติสำหรับตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย โดยกำหนดให้รหัสผ่านมีความยาวพอสมควร

(๒) ในการเปลี่ยนรหัสผ่านแต่ละครั้งจะต้องไม่กำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย

(๓) ระบบบริหารจัดการรหัสผ่านต้องป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้หรือที่จำเป็นต้องส่งไปในเครือข่ายเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๕.๔ การใช้งานโปรแกรมอรรถประโยชน์

(๑) ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมบางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๒) โปรแกรมอรรถประโยชน์ที่นำมาใช้งานต้องไม่ละเมิดลิขสิทธิ์

(๓) ต้องจัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน

(๔) ต้องยกเลิก ลบทิ้งโปรแกรมอรรถประโยชน์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงและใช้งานโปรแกรมอรรถประโยชน์ได้

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control) ต้องมีการควบคุมอย่างน้อย ดังนี้

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๖.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องดำเนินการ ดังนี้

(๑) แยกระบบซึ่งไวต่อการรบกวนออกจากระบบอื่น

(๒) การควบคุมสภาพแวดล้อมของระบบ

- แยกห้องติดตั้งระบบซึ่งไวต่อการรบกวนให้เป็นสัดส่วนเฉพาะ

- ควบคุมการเข้าออกห้องติดตั้งระบบซึ่งไวต่อการรบกวน โดยการกำหนดสิทธิการเข้าออกให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้องเท่านั้น

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบซึ่งไวต่อการรบกวน ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องดำเนินการ ดังนี้

(๑) ให้แต่งตั้งผู้รับผิดชอบเพื่อกำหนดสิทธิการในการเข้าถึงระบบควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๒) ได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

๖.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) กำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน ดังนี้

(๑) การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องได้รับอนุมัติจากผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน เป็นลายลักษณ์อักษรและต้องกำหนดระยะเวลาการเข้าถึงเพื่อควบคุมการเข้าถึงได้

(๒) การเข้าสู่ระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

(๓) ผู้ดูแลระบบต้องกำหนดมาตรการป้องกันและการเตรียมการต่าง ๆ ที่จำเป็นก่อนอนุญาตให้ผู้ใช้งานเริ่มต้นปฏิบัติงานจากระยะไกล

๖.๕ ลิขสิทธิ์ของซอฟต์แวร์และแนวทางป้องกันการละเมิดลิขสิทธิ์ของซอฟต์แวร์ที่ใช้งานในกรมการพัฒนาชุมชน ให้ผู้ดูแลระบบทั้งหน่วยงานราชการส่วนกลางและส่วนภูมิภาคปฏิบัติ ดังนี้

(๑) ในกรณีที่เจ้าหน้าที่มีความจำเป็นต้องใช้งานซอฟต์แวร์นอกเหนือจากที่กรมการพัฒนาชุมชนมีลิขสิทธิ์ ให้แจ้งความจำเป็นให้ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนพิจารณาความเหมาะสมและดำเนินการจัดซื้อให้ถูกต้อง

(๒) จัดทำทะเบียนคุมการติดตั้งซอฟต์แวร์บนคอมพิวเตอร์แม่ข่ายและลูกข่ายเพื่อตรวจสอบจำนวนลิขสิทธิ์และรายชื่อเครื่องคอมพิวเตอร์ที่มีการติดตั้งซอฟต์แวร์

(๓) เก็บเอกสารเกี่ยวกับลิขสิทธิ์ของซอฟต์แวร์อย่างเป็นระเบียบในสถานที่ปลอดภัย

(๔) ซอฟต์แวร์ที่ใช้งาน ต้องเป็นซอฟต์แวร์ที่ได้รับสิทธิการใช้งานถูกต้องตามกฎหมายหรือเป็นซอฟต์แวร์ที่ไม่สงวนลิขสิทธิ์

(๕) ซอฟต์แวร์ที่พัฒนาขึ้นหรือจัดจ้างให้มีการพัฒนาถือเป็นลิขสิทธิ์ของกรมการพัฒนาชุมชน ห้ามเจ้าหน้าที่นำไปเผยแพร่ต่อบุคคลภายนอก เว้นแต่ได้รับอนุญาตจากกรมการพัฒนาชุมชน

๖.๖ ซอฟต์แวร์สำเร็จรูป ในการติดตั้งซอฟต์แวร์สำเร็จรูปให้ผู้ติดตั้งซอฟต์แวร์ปฏิบัติ ดังนี้

(๑) ขอความเห็นชอบจากผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

(๒) ตรวจสอบไวรัสบนซอฟแวร์สำเร็จรูปก่อนการติดตั้ง

(๓) ติดตั้งซอฟต์แวร์สำเร็จรูปให้ครบถ้วนและทดสอบเพื่อให้แน่ใจว่าสามารถใช้งานได้อย่างมีประสิทธิภาพ

(๔) กรณีซอฟต์แวร์ที่ติดตั้ง

- มีคุณสมบัติด้านการรักษาความปลอดภัย ให้เลือกใช้งานคุณสมบัติดังกล่าวตามความเหมาะสมแก่การใช้งาน โดยซอฟต์แวร์ต้องมีความปลอดภัยและสามารถให้บริการได้ตามต้องการ

- ต้องกำหนดคุณสมบัติเฉพาะ เช่น ระบบป้องกันการบุกรุก เว็บเซิร์ฟเวอร์ เป็นต้น โดยให้ผู้จัดการฐานข้อมูลหน่วยงานราชการส่วนกลางและส่วนภูมิภาค ประสานงานกับกลุ่มงานพัฒนาระบบเครือข่าย ในการจัดทำเอกสารคู่มือของซอฟต์แวร์เพื่อใช้ประกอบการทำงานและปรับปรุงให้ถูกต้องทุกครั้งที่มีการเปลี่ยนแปลง ทั้งนี้ห้ามเปิดเผยเอกสารดังกล่าวต่อบุคคลผู้ไม่เกี่ยวข้อง เว้นแต่ได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

(๕) เอกสารคู่มือต้องแสดงรายละเอียดคุณสมบัติที่กำหนดเฉพาะสำหรับใช้งาน ได้แก่ คอมพิวเตอร์แม่ข่ายหรือเครื่องลูกข่ายที่ติดตั้งไดเรกทอรีที่จัดเก็บรายชื่อไฟล์ที่สำคัญและขั้นตอนการบริหารซอฟต์แวร์

๖.๗ ในกรณีจ้างเหมาดำเนินการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศให้ปฏิบัติ ดังนี้

(๑) ขอเห็นชอบจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) กรมการพัฒนาชุมชน

(๒) เอกสารคู่มือต้องแสดงคุณสมบัติที่กำหนดเฉพาะ ได้แก่ คอมพิวเตอร์แม่ข่ายหรือเครื่องลูกข่ายที่ติดตั้งไดเรกทอรีที่จัดเก็บรายชื่อไฟล์ที่สำคัญ และขั้นตอนการดำเนินการ

(๓) เทคโนโลยีสารสนเทศที่จัดจ้างให้มีการพัฒนาถือเป็นลิขสิทธิ์ของกรมการพัฒนาชุมชน ห้ามผู้รับจ้างนำไปเผยแพร่ต่อบุคคลภายนอก เว้นแต่ได้รับอนุญาตจากกรมการพัฒนาชุมชน

๗. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๗.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้ดูแลระบบหน่วยงานราชการส่วนกลาง หรือส่วนภูมิภาคที่ได้รับมอบหมาย

๗.๒ ผู้ดูแลระบบหน่วยงานราชการส่วนกลางและส่วนภูมิภาค ต้องดำเนินการดังต่อไปนี้

(๑) ลงทะเบียนกำหนดสิทธิผู้ใช้งานให้เหมาะกับหน้าที่ความรับผิดชอบ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

(๒) ต้องลงทะเบียนอุปกรณ์ทุกชิ้นที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๓) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายและป้องกันไม่ให้ผู้โจมตี สามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๔) ให้เปลี่ยนค่า SSID (Service Set Identifier) ทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(๕) ให้เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่าน ของอุปกรณ์ไร้สายและควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

(๖) ต้องกำหนดค่าใช้ WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

(๗) ให้เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ ที่มี MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น

(๘) ต้องทำการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

(๙) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอและเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการศูนย์สารสนเทศฯ ทราบโดยทันที

๗.๓ ผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของหน่วยงานราชการส่วนกลางและส่วนภูมิภาค มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

(๑) การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงานในแต่ละระดับและต้องกำหนดรหัสการเข้าใช้งาน

(๒) ห้ามนำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงานไม่ว่าจะเป็น Access Point, Wireless Routers, Wireless USB Client หรือ Wireless Card

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

(๔) กรณีที่หัวหน้าหน่วยงานอนุญาตให้มีการติดตั้ง Wireless ให้ดำเนินการ ดังนี้

- วาง Access Point (AP) ในตำแหน่งที่เหมาะสม โดยให้วางหน้า Firewall หากมีความจำเป็นต้องวางในระบบเครือข่ายภายใน (Internal Network) โดยให้เพิ่มการรับรองและการเข้ารหัสด้วย (Authentication, Encryption)

- ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้ Access Point ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น

- ให้จัดการกับ SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิต ค่า SSID ทันทีที่นำ Access Point มาใช้งาน และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัว Access Point ด้วย

- ผู้ดูแลระบบจะต้องเขียนการติดตั้ง Wireless อย่างถูกวิธีและปรับค่า Configuration ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

- อุปกรณ์ Wireless LAN ของแต่ละผู้ผลิตมีคุณสมบัติแตกต่างกัน ต้องตรวจสอบคุณสมบัติก่อนการใช้งาน

๘. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server)

๘.๑ ควบคุมการติดตั้งซอฟต์แวร์

(๑) ผู้ดูแลระบบ ต้องเป็นผู้ที่ได้รับการอบรมหรือมีความชำนาญเท่านั้น จึงมีมีสิทธิเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน

(๒) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องได้รับการอนุมัติก่อนดำเนินการ

(๓) ไม่ติดตั้งซอร์สโค้ด คอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

(๔) กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารี่สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๕) กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้อง ต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ เป็นต้น

(๖) ให้ผู้เกี่ยวข้องทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศให้ครบถ้วนก่อนให้บริการระบบสารสนเทศ

(๗) ให้จัดเก็บซอฟต์แวร์เวอร์ชั่นเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิมตามระยะเวลาที่เหมาะสม

(๘) ให้ระบุความต้องการด้านระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

๘.๒ ให้ทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ รวมทั้งวางแผนด้านงบประมาณในกรณีที่หน่วยงานต้องใช้ระบบปฏิบัติการใหม่และต้องแจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

๘.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

(๑) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในสินทรัพย์ทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์

(๒) ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๓) ให้ตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๘.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค

(๑) กำหนดให้จัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้นมีการบันทึก ดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชั่นที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟแวร์นั้น ๆ

(๒) กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมในทันที

(๓) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศให้ผู้ดูแลระบบดำเนินการ ดังนี้

- เฝ้าระวัง ติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

- กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่ นั้น

(๔) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๘.๕ ระบบตรวจจับและป้องกันผู้บุกรุก (Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) ผู้ดูแลระบบมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

(๑) เฝ้าระวังและรักษาอุปกรณ์ตรวจจับและป้องกันการบุกรุกระบบ รวมทั้งวิเคราะห์หาสาเหตุของการบุกรุก

(๒) เก็บสถิติเกี่ยวกับความพยายามบุกรุกหรือโจมตีองค์กรเพื่อเป็นเครื่องมือในการวัดประสิทธิภาพของระบบรักษาความปลอดภัยอื่นและเพื่อเป็นการป้องกันเครือข่ายคอมพิวเตอร์ถูกภัยคุกคามจากภายนอก เช่น Hacker รวมทั้งไวรัสประเภทต่าง ๆ

(๓) บริหารจัดการเหตุการณ์บุกรุกระบบ (Incident Management) เพื่อตอบสนองเหตุการณ์โดยวิเคราะห์ลักษณะการบุกรุก จัดลำดับความสำคัญของผลกระทบที่เกิดขึ้นกับองค์กรและจัดทำวิธีปฏิบัติเพื่อตอบสนองต่อเหตุการณ์การบุกรุก ต่อไปนี้

- จำกัดขอบเขต (Containment) ที่เสี่ยงต่อการบุกรุกและจำกัดความรุนแรงของการบุกรุก

- กำจัดต้นเหตุ (Eradication) รวมถึงปิดกั้นช่องทางของการบุกรุก

- กู้คืนระบบ (Recovery) แก้ไขระบบที่ถูกบุกรุกให้สามารถกลับมาทำงานได้ตามปกติ

- ติดตามผล (Follow-Up) บันทึกผลกระทบของเหตุการณ์และแนะนำวิธีปฏิบัติเพื่อป้องกันเหตุการณ์เกิดซ้ำ

(๔) กำหนดบุคคลรับผิดชอบการกำหนด แก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน รวมถึงการทบทวนอย่างน้อยปีละ ๑ ครั้ง และแจ้งผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนให้รับทราบเมื่อมีการเปลี่ยนแปลง

(๕) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อตรวจเช็คระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้มีอำนาจหน้าที่และจำกัดการใช้งานเฉพาะที่จำเป็น

(๖) ผู้ดูแลระบบต้องทำการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ ต้องประเมินผลกระทบของการเปลี่ยนแปลงที่สำคัญเป็นลายลักษณ์อักษร ทั้งในด้านการปฏิบัติงาน (Operation) ระบบรักษาความปลอดภัย (Security) และการทำงาน (Functionality) ของระบบงานที่เกี่ยวข้อง

๘.๖ การบันทึกข้อมูลจราจรคอมพิวเตอร์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) การบันทึกข้อมูลจราจรคอมพิวเตอร์ (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ข้อมูลชื่อบัญชีผู้ใช้งาน

(๒) ข้อมูลวันเวลาที่เข้าถึงและออกจากระบบ

(๓) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๔) ข้อมูลการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ

(๕) ข้อมูลความพยายามในการเข้าถึงสินทรัพย์สารสนเทศทั้งที่สำเร็จและไม่สำเร็จ

(๖) ข้อมูลการเปลี่ยนคอนฟิกกูเรชั่น (Configuration) ของระบบ

(๗) ข้อมูลแสดงการใช้งานแอพพลิเคชั่น

(๘) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

(๙) ข้อมูลไอพีแอดเดรสที่เข้าถึง

(๑๐) ข้อมูลโพรโตคอลเครือข่ายที่ใช้

(๑๑) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

(๑๒) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๘.๗ การเข้าถึงห้องคอมพิวเตอร์แม่ข่าย

(๑) ห้องคอมพิวเตอร์แม่ข่าย (Server) ที่ตั้งอยู่ ณ กรมการพัฒนาชุมชน สงวนไว้เป็นเขตหวงห้าม โดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

(๒) ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดของเครื่องออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

(๓) ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อประกอบธุรกิจส่วนบุคคล

๙. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อช่วยให้ผู้ใช้งานทั้งหน่วยงานราชการส่วนกลางและส่วนภูมิภาค ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ ดังนี้

๙.๑ ผู้ใช้งานต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานในทางที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ดังนี้

(๑) ทำให้แพร่หลาย ซึ่งข้อมูลคอมพิวเตอร์ที่อาจจะกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรหรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๕) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๖) นำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

(๗) เข้าถึงโดยมิชอบ ซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

(๘) นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

(๙) เข้าถึงโดยมิชอบ ซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน

(๑๐) กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

(๑๑) ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

(๑๒) กระทำด้วยประการใดโดยมิชอบเพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

(๑๓) ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (E-mail) แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

(๑๔) กระทำการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือการบริการสาธารณะหรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

๙.๒ ผู้ใช้งานต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตาม ๙.๑ (๑) - (๖) ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

๙.๓ ผู้ใช้งานต้องไม่จำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม ๙.๑ (๗) - (๑๔)

๙.๔ การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้ผู้ใช้งานปฏิบัติ ดังต่อไปนี้

(๑) ไม่คัดลอกโปรแกรมต่าง ๆ ที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๒) การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ของหน่วยงานจะต้องกำหนดโดยกรมการพัฒนาชุมชนเท่านั้น

(๓) ไม่ทำการปรับแต่งไบออส (BIOS) หรือการตั้งค่าระบบ (Configuration) อื่นใดที่อาจส่งผลกระทบต่อระบบการทำงานของคอมพิวเตอร์ อันเป็นเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้เป็นปกติ

(๔) ไม่ทำการเปลี่ยนแปลงเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์แบบตั้งโต๊ะภายในหน่วยงาน

(๕) หากผู้ใช้งานมีความประสงค์ขอใช้เลขที่อยู่ไอพีสาธารณะ (Public IP Address) ต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนเท่านั้น

(๖) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่มีความสามารถในการตรวจสอบข้อมูลบนระบบเครือข่าย

(๗) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานเพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานได้ เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

(๘) ไม่ใช้บริการบนระบบอินเทอร์เน็ต (Internet) ที่มีการครอบครองแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงาน

๙.๕ วิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use)

(๑) กำหนดชื่อผู้ใช้งานของทุกระบบงาน ตามวิธีปฏิบัติในการตั้งรหัสผ่านที่เหมาะสม ดังนี้

- ให้ตั้งชื่อผู้ใช้งานเป็นภาษาอังกฤษเท่านั้น
- รูปแบบการตั้งชื่อ ให้ใช้ชื่อผู้ใช้งานแล้วตามด้วยเครื่องหมาย Under Score (_) ตามด้วยนามสกุล ๓ ตัว ได้แก่ นายสมชาย ดีจริง Username = somchai_dee
- ในกรณีที่ชื่อนามสกุลเขียนภาษาอังกฤษแล้ว Username ซ้ำกันอีกให้เพิ่มอักษรนามสกุลออกไปได้อีก

(๒) ในการรักษาความปลอดภัยบัญชีผู้ใช้งาน การปฏิบัติตนเกี่ยวกับรหัสผ่าน ให้ผู้ใช้งานปฏิบัติ ดังนี้

- ไม่ตั้งรหัสผ่านโดยใช้ชื่อผู้ใช้งานในรูปแบบต่าง ๆ ได้แก่ กลับหน้าหลัง ใช้ตัวเลขหรือตัวอักษรที่เหมือนกันทั้งหมด
- ไม่ตั้งรหัสผ่านโดยใช้ชื่อหรือข้อมูลต่าง ๆ ที่เกี่ยวข้องผู้ใช้งาน ได้แก่ ชื่อ นามสกุล วันเกิด ชื่อบุตร หมายเลขโทรศัพท์
- ไม่ตั้งรหัสผ่านโดยใช้คำที่อยู่ในพจนานุกรม
- รหัสผ่านต้องมีความยาวเกิน ๖ ตัวอักษร
- ตั้งรหัสผ่านที่ผสมระหว่างอักษรตัวเล็กและอักษรตัวใหญ่
- รหัสผ่านที่ผสมกับอักขระพิเศษ (; $ เป็นต้น)
- ในกรณีที่ระบบรองรับการเปลี่ยนรหัสผ่านให้เปลี่ยนรหัสผ่านโดยไม่ชักช้า เมื่อเข้าใช้งานระบบในครั้งแรก
- ห้ามเปิดเผยรหัสผ่านแก่ผู้อื่นและไม่จดรหัสผ่านลงกระดาษหรือสื่ออื่น ๆ หรือกำหนดให้เครื่องคอมพิวเตอร์จำรหัสผ่าน หากเกิดความเสียหายเจ้าของรหัสผ่านต้องรับผิดชอบ
- หากมีความจำเป็นต้องเปิดเผยรหัสผ่านให้ผู้อื่นใช้งานจะต้องควบคุมดูแลอย่างใกล้ชิดเพื่อไม่ให้เกิดความเสียหายต่อกรมการพัฒนาชุมชน
- เปลี่ยนรหัสผ่านอย่างน้อยทุก ๖๐ วัน

(๓) หากสงสัยว่าบุคคลอื่นลักลอบหรืออาจลักลอบใช้บัญชีผู้ใช้งานหรือสงสัยว่ามีการละเมิดการรักษาความปลอดภัยบัญชีผู้ใช้งาน ให้แจ้งผู้ดูแลระบบเปลี่ยนรหัสผ่านโดยไม่ชักช้า

(๔) ในกรณีลืมรหัสผ่านให้แจ้งผู้ดูแลระบบโดยตรงเพื่อสร้างรหัสผ่านใหม่

(๕) ในกรณีถูกยกเลิกสิทธิการใช้งานชั่วคราวละประสงค์จะขอคืนสิทธิการใช้งาน ให้แจ้งผู้ดูแลระบบเพื่อขอบัญชีผู้ใช้งานเป็นลายลักษณ์อักษรและยื่นหลักฐานดังกล่าวต่อผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

(๖) ในกรณีมีบุคลากรลาออกและประสงค์จะใช้บัญชีผู้ใช้งานต่อเป็นการชั่วคราว ให้แจ้งผู้ดูแลระบบเป็นลายลักษณ์อักษรเพื่อพิจารณาและยื่นหลักฐานดังกล่าวต่อผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

(๗) ผู้ดูแลระบบต้องเปลี่ยนรหัสถี่กว่าผู้ใช้งานทั่วไป

๙.๖ วิธีปฏิบัติเพื่อป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานเพื่อป้องกันผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(๑) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๒) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๑๐ นาที และกำหนดให้ใส่รหัสผ่านจึงจะสามารถเปิดหน้าจอได้

(๓) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๙.๗ วิธีปฏิบัติเพื่อควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

(๑) ข้อปฏิบัติในการป้องกันและควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศให้อยู่ในสถานที่ที่ปลอดภัย ดังนี้

- จำกัดการเข้าถึงสินทรัพย์สารสนเทศที่สำคัญให้กำหนดสิทธิเฉพาะบุคคลที่เกี่ยวข้อง
- การจัดบริเวณการเข้าถึงบุคคลภายนอก
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร
- ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ทำลายสื่ออิเล็กทรอนิกส์ ตามภาคผนวก ก เพื่อป้องกันการนำกลับมาใช้ใหม่

(๒) การป้องกันต้องมีความสอดคล้องกับประเด็นต่าง ๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับหรือข้อกำหนดอื่น ๆ
- วัฒนธรรมองค์กร

(๓) การป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

๙.๘ ให้ผู้ใช้งานนำการเข้ารหัส (Encryption) มาใช้กับข้อมูลที่เป็นความลับ โดยจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๑๐. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา (Use of Personal Computers and Portable Computers)

๑๐.๑ การใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงาน ดังนั้น ต้องใช้งานอย่างมีประสิทธิภาพเพื่อบรรลุเป้าหมายของหน่วยงาน

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) การตั้งชื่อคอมพิวเตอร์ (Computer Name) ต้องเป็นไปตามที่กรมการพัฒนาชุมชนกำหนด

(๔) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งแก้ไขหรือเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน

(๕) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องดำเนินการโดยผู้ดูแลระบบหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น

(๖) การกำหนดสิทธิให้ผู้อื่นสามารถเห็นไฟล์ในเครื่องคอมพิวเตอร์ (File Sharing) ผู้ใช้งานต้องกระทำอย่างระมัดระวัง โดยกำหนดสิทธิเฉพาะบุคคลที่จำเป็น

(๗) ผู้ใช้งานต้อง Shut Down คอมพิวเตอร์ส่วนบุคคลทุกครั้งหลังเลิกใช้งานในแต่ละวัน เพื่อป้องกันระบบปฏิบัติการเสียหาย

(๘) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องทำการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสที่หน่วยงานจัดหาให้เท่านั้น

(๙) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่

(๑๐) ไม่นำอาหารหรือเครื่องดื่มเข้าใกล้บริเวณเครื่องคอมพิวเตอร์ตั้งอยู่

(๑๑) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

(๑๒) ห้ามใช้หรือวางเครื่องคอมพิวเตอร์ และอุปกรณ์แบบพกพาในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า ๓๕ องศาเซลเซียส

(๑๓) ผู้ใช้งาน มีหน้าที่ป้องกันการสูญหายของเครื่องคอมพิวเตอร์และอุปกรณ์แบบพกพา

๑๐.๒ การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานต้องประเมินความเสี่ยงว่า ข้อมูลที่เก็บไว้บน Hard Disk เป็นข้อมูลที่ไม่สำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

๑๐.๓ การใช้คอมพิวเตอร์ส่วนบุคคล

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลของตนเองที่จัดเก็บในคอมพิวเตอร์ส่วนบุคคลเพื่อใช้กู้คืนข้อมูลในกรณีที่เครื่องคอมพิวเตอร์ได้รับความเสียหาย

(๒) การป้องกันไวรัส ให้ผู้ใช้งานปฏิบัติ ดังนี้

- ปรับปรุงหรือตรวจสอบการปรับปรุงเวอร์ชั่นของซอฟต์แวร์ตรวจสอบไวรัสทุกครั้งที่ได้รับแจ้งจากศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

- ในกรณีที่นำแผ่นดิสก์จากผู้อื่นหรือคัดลอกไฟล์จากเครื่องอื่นมาใช้งานคอมพิวเตอร์ส่วนบุคคล ให้ตรวจสอบไวรัสก่อนการใช้งานทุกครั้ง

(๓) ให้ผู้ใช้งานตั้งรหัสผ่านที่โปรแกรมรักษาหน้าจอ (Screen Saver) เพื่อป้องกันบุคคลอื่นลักลอบใช้งานหรือดูข้อมูลในเครื่องคอมพิวเตอร์ในขณะที่ผู้ใช้งานไม่อยู่หน้าเครื่อง

(๔) ผู้ใช้งานไม่แก้ไขการกำหนดค่าเกี่ยวกับเครือข่ายหรือฮาร์ดแวร์ของคอมพิวเตอร์ส่วนบุคคลด้วยตนเอง ในกรณีที่มีความจำเป็นต้องแก้ไขให้ปรึกษาศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

๑๐.๔ คอมพิวเตอร์แบบพกพา

(๑) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน

(๒) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๓) การเคลื่อนย้ายขณะที่เครื่องเปิดใช้งานอยู่ ให้ยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้นโดยเด็ดขาด

(๔) ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่างๆ เป็นต้น

(๕) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๖) ห้ามผู้ใช้งานเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

๑๑. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ (Management of Confidential Data Access)

๑๑.๑ การรักษาความปลอดภัยข้อมูล แบ่งออกเป็น ๒ ประเภท คือ

(๑) ข้อมูลลับที่สุด ข้อมูลลับมาก ข้อมูลลับ ได้แก่ ข้อมูลที่ถูกกำหนดชั้นความลับตามหลักเกณฑ์เกี่ยวกับการรักษาความปลอดภัยของบุคคลและเอกสารที่กรมการพัฒนาชุมชนกำหนดหรือถือปฏิบัติอยู่ในเวลานั้น

(๒) ข้อมูลทั่วไป ได้แก่ ข้อมูลที่ไม่ถูกกำหนดชั้นความลับ

๑๑.๒ เพื่อประโยชน์ในการรักษาความปลอดภัยข้อมูล ให้ศูนย์สารสนเทศเพื่อการพัฒนาชุมชนดำเนินการดังต่อไปนี้

(๑) กำหนดวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานเพื่อป้องกันการลักลอบเข้าถึงข้อมูล

(๒) กำหนดวิธีปฏิบัติในการจัดเก็บข้อมูลแต่ละประเภทเพื่อป้องกันการลักลอบดูข้อมูลและแก้ไขข้อมูล

(๓) กำหนดวิธีปฏิบัติในการรับส่งข้อมูลแต่ละประเภทเพื่อป้องกันการลักลอบดูข้อมูลหรือสร้างความเสียหายให้กับข้อมูลในระหว่างรับส่ง

(๔) กำหนดวิธีปฏิบัติในการทำลายข้อมูลแต่ละประเภท เมื่อข้อมูลหมดอายุการใช้งานหรือมีความจำเป็นต้องทำลายเพื่อป้องกันการลักลอบดูข้อมูลที่ค้างในอุปกรณ์เฉพาะสำหรับจัดเก็บ

(๕) กำหนดวิธีปฏิบัติในการสำรองข้อมูลแต่ละประเภทให้เหมาะสมกับจำนวนครั้งในการเปลี่ยนแปลงของข้อมูลเพื่อใช้กู้คืนในกรณีที่ข้อมูลได้รับความเสียหายและให้เก็บสื่อที่ใช้สำรองข้อมูลในอุปกรณ์เฉพาะสำหรับจัดเก็บที่มีความปลอดภัย

๑๑.๓ เจ้าของข้อมูลต้องทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๑๑.๔ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

๑๑.๕ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

๑๑.๖ ให้หน่วยราชการส่วนกลางและส่วนภูมิภาค มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน ต้องมีการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๑๑.๗ วิธีปฏิบัติที่เกี่ยวข้องกับข้อมูลลับบนอุปกรณ์คอมพิวเตอร์ ให้ถือปฏิบัติตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐

(๑) การทำลายข้อมูลลับให้เป็นไปตามคำสั่ง เรื่อง การรักษาความปลอดภัยเกี่ยวกับบุคคลและข้อมูลข่าวสารลับ โดยวิธีการทำลายข้อมูลลับให้ปฏิบัติตามวิธีปฏิบัติตามภาคผนวก ก

(๒) ในการสำรองข้อมูลลับ ให้ปฏิบัติ ดังนี้

- สำรองข้อมูลตามระยะเวลาที่ศูนย์สารสนเทศเพื่อการพัฒนาชุมชนกำหนดหรือเมื่อได้รับแจ้งจากเจ้าของข้อมูลว่าข้อมูลมีการเปลี่ยนแปลงจากเดิมอย่างเป็นนัยสำคัญ
- จัดเก็บสื่อที่ใช้สำรองข้อมูลในอุปกรณ์เฉพาะสำหรับเก็บรักษาที่ปิดล็อคได้
- ตรวจสอบความครบถ้วนของข้อมูลที่สำรองทุกครั้ง

๑๑.๘ การควบคุมการเข้าถึงข้อมูลทั่วไปให้หน่วยราชการส่วนกลางและส่วนภูมิภาค กำหนดให้เจ้าของข้อมูลหรือผู้ได้รับมอบหมายทำหน้าที่บริหารความปลอดภัยของข้อมูล ดังนี้

(๑) เจ้าของไฟล์ข้อมูลสามารถอ่านและเขียนไฟล์ข้อมูลและบุคคลทั่วไปสามารถอ่านไฟล์ข้อมูลได้เท่านั้น

(๒) กรณีข้อมูลที่จัดเก็บในฐานข้อมูลควรกำหนดให้ผู้ใช้งานสามารถเข้าถึงข้อมูลในฐานข้อมูลผ่านระบบงานเท่านั้น ไม่ควรให้เข้าถึงข้อมูลในฐานข้อมูลโดยตรง

(๓) วิธีการทำลายข้อมูลทั่วไปควรปฏิบัติตามวิธีปฏิบัติในภาคผนวก ก

(๔) การสำรองข้อมูลทั่วไปให้หน่วยราชการส่วนกลางและส่วนภูมิภาคเจ้าของข้อมูลหรือหน่วยงานอื่นที่ได้รับมอบหมายจากเจ้าของข้อมูลให้ทำหน้าที่บริหารความปลอดภัยของข้อมูลให้ปฏิบัติ ดังนี้

- สำรองข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อยหรือเมื่อได้รับแจ้งจากเจ้าของข้อมูลว่าข้อมูลมีการเปลี่ยนแปลงจากเดิมอย่างเป็นนัยสำคัญ
- ควรจัดเก็บสื่อที่ใช้สำรองข้อมูลลงบน แผ่น CD แผ่น DVD HardDisk
- ควรตรวจสอบความครบถ้วนของข้อมูลที่สำรองทุกครั้ง

๑๒. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๒.๑ ระบบจดหมายอิเล็กทรอนิกส์ของกรมการพัฒนาชุมชน มีวัตถุประสงค์เพื่อการใช้งานของกรมการพัฒนาชุมชนเท่านั้น ห้ามนำบัญชีจดหมายอิเล็กทรอนิกส์ (E-Mail Account) ไปใช้นอกเหนือจากวัตถุประสงค์ที่หน่วยงานกำหนด

๑๒.๒ ให้หน่วยราชการส่วนกลางและส่วนภูมิภาค นำกฎระเบียบข้อบังคับการส่งและรับจดหมายอิเล็กทรอนิกส์ผ่านอินเทอร์เน็ตเพื่อใช้เป็นแนวทางให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) การส่งจดหมายอิเล็กทรอนิกส์

- การส่งข้อมูลแนบที่มีความเสี่ยงต่อความเสียหายให้เข้ารหัสก่อน
- การส่งจดหมายอิเล็กทรอนิกส์ ๑ ฉบับ ห้ามส่งไฟล์แนบที่มีขนาดเกิน ๒๕ MB และต้องบีบอัดไฟล์แนบก่อนส่ง
- ห้ามใช้จดหมายอิเล็กทรอนิกส์ของกรมการพัฒนาชุมชนเพื่อเจตนาสร้างความเสียหายให้กับผู้อื่น เช่น ส่งจดหมายอิเล็กทรอนิกส์ซ้ำหลายครั้ง ข้อมูลลักษณะลูกโซ่ ส่งข้อความเท็จหรือข้อความพาดพิงถึงบุคคลอื่น เป็นต้น
- ไม่ส่งข้อความทางจดหมายอิเล็กทรอนิกส์ที่มีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

(๒) การรับจดหมายอิเล็กทรอนิกส์

- ลบจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้งานอย่างสม่ำเสมอเพื่อไม่ให้เนื้อที่ในการจัดเก็บจดหมายอิเล็กทรอนิกส์เต็ม
- ไม่ควรเปิดเมล์ ไฟล์แนบหรือคลิกลิงค์ที่ไม่เกี่ยวข้องกับงานของกรมการพัฒนาชุมชน
- ในกรณีที่สงสัยว่ามีการใช้จดหมายอิเล็กทรอนิกส์ที่ผิดปกติเกิดขึ้น เช่น ได้รับจดหมายอิเล็กทรอนิกส์ฉบับเดียวกันซ้ำหลายครั้งหรือได้รับจดหมายอิเล็กทรอนิกส์จากบุคคลที่ไม่รู้จักเป็นประจำ เป็นต้น ควรรีบแจ้งศูนย์สารสนเทศเพื่อการพัฒนาชุมชนเพื่อดำเนินการตรวจสอบ

(๓) การใช้หมายเลขไปรษณีย์อิเล็กทรอนิกส์

- การแจ้งหมายเลขไปรษณีย์อิเล็กทรอนิกส์ของกรมการพัฒนาชุมชน สามารถทำได้ในกรณีที่ต้องติดต่องานของหน่วยงานหรือรู้จักบุคคลหรือองค์กรดังกล่าวเป็นอย่างดี

- ในกรณีที่มีความจำเป็นต้องติดต่อเรื่องส่วนตัวกับบุคคลหรือองค์กรที่ไม่รู้จักควรใช้หมายเลขไปรษณีย์อิเล็กทรอนิกส์อื่น

๑๒.๓ แนวทางการควบคุมการใช้งาน ให้ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนดำเนินการ ดังนี้

(๑) กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน

(๒) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๕ ครั้ง

(๓) ทบทวนสิทธิการเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(๔) การควบคุมการเข้าถึงระบบตามแนวทางการบริหารจัดการเข้าถึงผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้อย่างเคร่งครัด

๑๒.๔ การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ คู่สัญญาหรือตามภารกิจของกรมการพัฒนาชุมชน ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมการพัฒนาชุมชนเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของกรมการพัฒนาชุมชนขัดข้องและได้รับการอนุญาตจากผู้มีอำนาจแล้วเท่านั้น

๑๒.๕ การใช้งานจดหมายอิเล็กทรอนิกส์ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

๑๒.๖ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของกรมการพัฒนาชุมชนเพื่อส่งจดหมายอิเล็กทรอนิกส์ที่ไม่ได้มีวัตถุประสงค์ในงานภารกิจของกรมการพัฒนาชุมชนหรือส่งจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาเรื่องส่วนตัว หากผู้ใช้งานต้องการส่งจดหมายอิเล็กทรอนิกส์ดังกล่าว ขอให้ใช้งานจากบริการจดหมายอิเล็กทรอนิกส์ฟรี

๑๒.๗ ห้ามผู้ใช้งานนำบัญชีจดหมายอิเล็กทรอนิกส์ (E-Mail Account) ซึ่งเป็นของกรมการพัฒนาชุมชนไปเผยแพร่สู่บุคคลอื่นไม่ว่าจะเป็นทางใดก็ตาม เช่น การโพสต์ในเว็บบอร์ดในชุดคำถามหรือแบบสอบถามจากผู้ค้า เป็นต้น เว้นแต่การเผยแพร่นั้นเป็นไปเพื่อผลประโยชน์ทางราชการ หรือได้รับอนุญาตจากผู้มีอำนาจแล้วเท่านั้น

๑๒.๘ การส่งจดหมายอิเล็กทรอนิกส์ผู้ใช้งานต้องระบุชื่อผู้รับ หัวข้อ ให้ชัดเจน และใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ปลุกปั่น ยั่วยุ เสียดสี หรือส่อในทางผิดกฎหมาย

๑๒.๙ ผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของกรมการพัฒนาชุมชน หรือก่อให้เกิดความเสียหายต่อกรมการพัฒนาชุมชน

๑๒.๑๐ ห้ามใช้จดหมายอิเล็กทรอนิกส์ของกรมการพัฒนาชุมชนเพื่อเผยแพร่ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมายหรือกระทบต่อการดำเนินงาน ตลอดจนการรบกวนผู้ใช้งานอื่นหรือผู้รับบริการของกรมการพัฒนาชุมชน

๑๓. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๓.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

๑๓.๒ ผู้ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัย รวมถึงพฤติกรรมที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

๑๓.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับหน่วยงาน ผู้ใช้งานต้องแจ้งต่อศูนย์สารสนเทศเพื่อการพัฒนาชุมชนโดยเร็วที่สุดเพื่อดำเนินการตามความเหมาะสม

๑๔. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ให้ปฏิบัติดังต่อไปนี้

๑๔.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

๑๔.๒ ห้ามแก้ไขข้อมูลจราจรทางคอมพิวเตอร์ (Log)

๑๔.๓ หากต้องการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Log) ต้องได้รับการอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

๑๔.๔ กำหนดให้บันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า - ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

๑๔.๕ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑๕. การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Malware)

๑๕.๑ คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสของคอมพิวเตอร์ (Antivirus) ตามที่กรมได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องมือเพื่อการศึกษาพัฒนาระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บังคับบัญชาผู้ที่ได้รับมอบหมาย

๑๕.๒ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๑๕.๓ ผู้ใช้งานต้องทำการปรับปรุงข้อมูลเพื่อตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอเพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

๑๕.๔ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

๑๕.๕ เมื่อผู้ใช้งานพบว่า เครื่องคอมพิวเตอร์ติดไวรัสผู้ใช้งานต้องไม่เชื่อมต่อคอมพิวเตอร์เข้าสู่เครือข่ายและต้องแจ้งแก่ผู้ดูแลระบบ

๑๕.๖ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสารหรือสิ่งใด ๆ ที่เป็นทรัพย์สินของกรมหรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

๑๕.๗ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของกรม

๑๕.๘ กรณีที่คอมพิวเตอร์หรือระบบมีปัญหาผู้ใช้งานต้องทำการสำรองข้อมูลที่จำเป็นของผู้ใช้งานเองก่อนที่จะทำการก็คืนหรือตรวจสอบแก้ไขระบบ

๑๖. การป้องกันโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

๑๖.๑ ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการเว็บบราวเซอร์และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๑๖.๒ ห้ามผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

๑๖.๓ หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องเข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่นๆ ได้

๑๗. การบริหารระบบรักษาความปลอดภัยไฟร์วอลล์ (Firewall)

วัตถุประสงค์เพื่อควบคุมการสื่อสารระหว่างเครือข่ายภายในกรมกับเครือข่ายภายนอกกรม โดยการตั้งค่าของไฟร์วอลล์และอุปกรณ์ที่อนุญาตให้เชื่อมโยงภายในกรมให้มีประสิทธิภาพในการทำงาน รวมทั้งต้องทบทวนสิทธิของผู้ใช้งานอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบไฟร์วอลล์

แนวทางปฏิบัติ

(๑) ผู้ดูแลระบบมีหน้าที่ในการบริหารจัดการระบบรักษาความปลอดภัยไฟร์วอลล์ทั้งหมด

(๒) ผู้ดูแลระบบต้องกำหนดนโยบาย (Policy) การใช้งานไฟร์วอลล์

(๓) ผู้ดูแลระบบต้องกำหนดค่า (Configuration) หรือกำหนดนโยบาย (Policy) เพื่อกลั่นกรองข้อมูลและระบบความปลอดภัยของระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ของกรม การป้องกันการบุกรุกไวรัส รวมทั้ง Malicious Code ต่างๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์

(๔) ผู้ดูแลระบบต้องกำหนดขั้นตอนหรือวิธีการปฏิบัติในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะผิดปกติต้องดำเนินการแก้ไขและรายงานผู้บังคับบัญชาโดยทันที

(๕) ผู้ดูแลระบบต้องเปิดใช้งานไฟร์วอลล์ตลอดเวลา

(๖) การเปิดใช้บริการ Service ต้องรับอนุญาตจากผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ผู้ดูแลระบบต้องกำหนดมาตรการป้องกันเพิ่มเติม

(๗) ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาตต้องบันทึกการเปลี่ยนแปลงทุกครั้ง

(๘) การเข้าถึงกระบวนการไฟร์วอลล์ต้องเข้าได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

(๙) ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้า - ออกอุปกรณ์ไฟร์วอลล์ ต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์และต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๖๐ วัน

(๑๐) การกำหนดค่าการบริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่ใช้งานเท่านั้น โดยนโยบายต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

(๑๑) ต้องสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์และทุกครั้งที่มีการเปลี่ยนแปลงค่า

(๑๒) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ ต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยกำหนดเป็นกรณีไป

(๑๓) ผู้ดูแลระบบมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

(๑๔) การเชื่อมต่อในลักษณะของการ Remote login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายในต้องการทำผ่าน VPN เท่านั้น และต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายและต้องได้รับความเห็นชอบจากผู้ดูแลระบบ

(๑๕) ผู้ละเมิดนโยบายความปลอดภัยของไฟร์วอลล์ ต้องถูกระงับการใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ทันที

(๑๖) ผู้ขอใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน โดยระบุข้อมูล ดังนี้

- หมายเลข Port ที่ต้องการเปิด
- หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร
- วัตถุประสงค์หรือ Application ที่ต้องการใช้งานผ่าน Port นั้น ๆ
- วันที่เริ่มใช้และวันที่สิ้นสุดการใช้

(๑๗) ในการขอใช้งาน หากพบว่าขัดต่อนโยบาย ประกาศ ระเบียบของกรม หรือกฎหมาย หรืออาจเกิดช่องโหว่ด้านความปลอดภัยของระบบสารสนเทศ ศูนย์สารสนเทศเพื่อการพัฒนาชุมชนจะไม่อนุญาตให้ใช้งาน

(๑๘) ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานขัดต่อนโยบาย ประกาศ ระเบียบของกรม หรือกฎหมายหรืออาจเกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศสารสนเทศ ศูนย์สารสนเทศเพื่อการพัฒนาชุมชนต้องยกเลิกการให้บริการทันที

ส่วนที่ ๒

นโยบายระบบสารสนเทศ และระบบสำรองของสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ผู้ใช้งานระบบสารสนเทศของกรมการพัฒนาชุมชน ได้รับทราบถึงข้อห้ามและข้อปฏิบัติที่จะส่งผลให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศและเกิดการใช้งานตรงตามวัตถุประสงค์การใช้งานระบบสารสนเทศของกรมการพัฒนาชุมชน รวมทั้งไม่ละเมิดระเบียบ กฎหมายหรือทำให้เกิดความเสียหายในการปฏิบัติงาน

๒. เพื่อให้ระบบสารสนเทศของหน่วยงานให้บริการได้อย่างต่อเนื่อง

๓. เพื่อเป็นมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานเป็นไปอย่างเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) กรมการพัฒนาชุมชน
๒. ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน กรมการพัฒนาชุมชน
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. ผู้ดูแลระบบต้องพิจารณาคัดเลือกระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้ โดยมีหลักเกณฑ์พิจารณา ดังนี้

๑.๑ การควบคุมสภาพแวดล้อมที่เหมาะสมและมีระบบสำรองที่เพียงพอ
๑.๒ มีความสอดคล้องกับเทคโนโลยี
๑.๓ ประเมินความเสี่ยงยอมรับได้โดยเจ้าของระบบงาน

๒. ผู้ดูแลระบบต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสม ให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๒.๑ ให้ผู้ดูแลระบบจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรองและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๒ ให้ผู้ดูแลระบบสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้และความถี่ในการสำรอง
- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูลผ่านระบบสำรอง ได้แก่ ข้อมูล วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลการกำหนดคุณสมบัติของคอมพิวเตอร์ (Configuration) ข้อมูลในฐานข้อมูล เป็นต้น
- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงวันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบไว้อย่างชัดเจน
- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น
- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
- ทดสอบบันทึกข้อมูลสำรอง อย่างน้อยปีละ ๑ ครั้ง เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- จัดทำขั้นตอนปฏิบัติสำเร็จการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างน้อยปีละ ๑ ครั้ง
- กำหนดให้ใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๓. จัดทำแผนเตรียมความพร้อม กรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อม กรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจและแนวทางต่อไปนี้

๓.๑ จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) กำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) ประเมินความเสี่ยงสำเร็จระบบที่มีความสำคัญเหล่านั้นและกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุม ประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่ายฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๓.๒ ทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๔. หน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรองและการจัดทำแผนเตรียมพร้อมกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ การจัดองค์กรปฏิบัติการฉุกเฉินและกำหนดผู้รับผิดชอบในระบบสารสนเทศกรมการพัฒนาชุมชนเมื่อเกิดเหตุฉุกเฉิน ดังนี้

๔.๑ <u>ระดับนโยบาย</u> ได้แก่

(๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

(๒) ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

<u>รับผิดชอบ</u> ในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ

๔.๒ ระดับอำนวยการ ได้แก่ ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

<u>รับผิดชอบ</u>

- เป็นผู้บังคับบัญชาสูงสุดในการควบคุมและปฏิบัติการฉุกเฉินระบบสารสนเทศ
- มีอำนาจสั่งการให้ทุกหน่วยหยุดหรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศกรมการพัฒนาชุมชน
- กำหนดจุดปลอดภัยสำหรับบุคคลและวัสดุอุปกรณ์ต่างๆ ในสถานที่ที่เหมาะสม
- ประชุมหารือกับผู้จัดการฐานข้อมูล
- ประเมินสถานการณ์และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม
- รายงานข้อมูลและผลการปฏิบัติงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบ

๔.๓ ระดับประสานงานเหตุฉุกเฉิน ได้แก่

(๑) ผู้อำนวยการกลุ่มงานพัฒนาระบบเทคโนโลยี

(๒) ผู้อำนวยการกลุ่มงานพัฒนาระบบเครือข่าย

<u>รับผิดชอบ</u>

- วิเคราะห์สถานการณ์ในที่เกิดเหตุแล้วแจ้งเหตุต่อผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนเพื่อระงับเหตุฉุกเฉิน
- มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่าผู้อำนวยศูนย์สารสนเทศเพื่อการพัฒนาชุมชนจะมาถึงที่เกิดเหตุ
- มีอำนาจสั่งการแทนผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน ในกรณีที่ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน ไม่สามารถสั่งการได้
- สั่งการให้เจ้าหน้าที่ผู้เกี่ยวข้องมาปฏิบัติการตามแผนฯ

- พิจารณาขั้นตอนและวิธีการป้องกันชีวิต ทรัพย์สิน ให้เสียหายน้อยที่สุด

- กำหนดอัตรากำลังพล วัสดุอุปกรณ์และเครื่องมือจำเป็นต้องขอเพิ่มเติมในอนาคต

๔.๔ ระดับหัวหน้าสั่งการ ณ ที่เกิดเหตุ

(๑) ผู้อำนวยการกลุ่มงานพัฒนาระบบเครือข่าย

(๒) ผู้อำนวยการกลุ่มงานระบบสารสนเทศชุมชน

(๓) ผู้อำนวยการกลุ่มงานพัฒนาระบบเทคโนโลยี

<u>รับผิดชอบ</u>

- กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษา ทบทวน วางแผนติดตาม การบริหารความเสี่ยงและระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

- แจ้งเหตุฉุกเฉินและเคลื่อนย้ายตนเอง ผู้อื่น ตลอดจนทรัพย์สินออกจากที่เกิดเหตุไปเก็บรักษา ณ จุดปลอดภัยโดยเร็ว

- ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชนและเจ้าหน้าที่ประสานงานรักษาความปลอดภัยทราบ

- นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพและรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

๔.๕ ระดับทีมงานที่เกี่ยวข้องกับแผน

(๑) ทีมรับผิดชอบดูแลบำรุงรักษาข้อมูลสารสนเทศ มีหน้าที่เฝ้าระวังและตรวจสอบ บำรุงรักษาแก้ไขข้อบกพร่องต่าง ๆ ของข้อมูลพื้นฐาน รวมทั้งการทำสำเนาและกู้คืนข้อมูลพื้นฐาน ผู้อำนวยการกลุ่มงานข้อมูลพื้นฐานการพัฒนาชนบทรับผิดชอบกำกับดูแล

(๒) ทีมรับผิดชอบดูแลระบบโปรแกรมสารสนเทศ มีหน้าที่เฝ้าระวังและตรวจสอบบำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของระบบโปรแกรมสารสนเทศ รวมทั้งทำสำเนาและกู้คืนฐานข้อมูลสารสนเทศ ผู้อำนวยการกลุ่มงานระบบสารสนเทศชุมชนรับผิดชอบกำกับดูแล

(๓) ทีมรับผิดชอบดูแลระบบเทคโนโลยีคอมพิวเตอร์ มีหน้าที่เฝ้าระวังและตรวจสอบบำรุงรักษาแก้ไขข้อบกพร่องต่างๆ ของระบบเทคโนโลยีคอมพิวเตอร์ รวมทั้งดำเนินตามแผนรองรับสถานการณ์ฉุกเฉิน ผู้อำนวยการกลุ่มงานพัฒนาระบบเทคโนโลยีรับผิดชอบกำกับดูแล

(๔) ทีมรับผิดชอบดูแลระบบเครือข่าย มีหน้าที่เฝ้าระวังและตรวจสอบบำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของระบบเครือข่าย รวมทั้งการทำสำเนาและกู้คืนฐานข้อมูลบนระบบคอมพิวเตอร์แม่ข่าย ผู้อำนวยการกลุ่มงานพัฒนาระบบเครือข่ายรับผิดชอบกำกับดูแล

๕. ทดสอบและทบทวนสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉิน สภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓

นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ
๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) กรมการพัฒนาชุมชน
๒. ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน กรมการพัฒนาชุมชน
๓. ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)
๔. ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้

๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. แนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

๒.๑ ให้ทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๒.๒ ให้ทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๒.๓ ให้ตรวจสอบและประเมินความเสี่ยงความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อการธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง (Integrity) ความพร้อมใช้ (Availability) และให้จัดทำรายงานพร้อมข้อเสนอแนะต่อผู้บริหาร อย่างน้อยปีละ ๑ ครั้ง

๒.๔ มาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้ระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) ให้เฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Log) แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ จัดเก็บข้อมูลตามข้อ ๑๔

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนาและมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๔

นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของกรมการพัฒนาชุมชน

๒. เพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน

๓. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) กรมการพัฒนาชุมชน

๒. ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน กรมการพัฒนาชุมชน

๓. ผู้อำนวยการสถาบันการพัฒนาชุมชน

๔. ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

แนวปฏิบัติ

๑. จัดฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๒. จัดทำคู่มือการใช้งานระบบสารสนเทศและมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน

๓. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

๔. จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและเสริมสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดให้ความรู้

๕. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

๖. ระดมการมีส่วนร่วมและภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผลและสำรวจความต้องการของผู้ใช้งาน

ส่วนที่ ๕

การพิจารณาความผิด และการดำเนินการทางวินัย

ความผิด

ผู้ใช้งานระบบคอมพิวเตอร์กรมการพัฒนาชุมชน ที่มีเจตนาฝ่าฝืนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการพัฒนาชุมชน แม้ว่าการฝ่าฝืนนั้นจะกระทำไม่บรรลุผลโดยสมบูรณ์ก็ให้ถือว่ามีความผิดโดยสมบูรณ์

การลงโทษ

ความผิดเกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการพัฒนาชุมชน ให้ลงโทษผู้มีเจตนาฝ่าฝืนตามระเบียบและกฎหมายที่เกี่ยวข้อง

การบังคับใช้

กำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้บังคับใช้นโยบายนี้ โดยให้ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับหน่วยงาน ต้องยึดถือแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมการพัฒนาชุมชน เป็นแนวทางในการปฏิบัติงานโดยเคร่งครัด

กรณี ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมากจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความปลอดภัยด้านสารสนเทศ กำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ภาคผนวก ก.

ภาคผนวก ก

วิธีปฏิบัติในการทำลายข้อมูล

อุปกรณ์สำหรับจัดเก็บ	วิธีทำลายข้อมูล
แผ่นดิสก์	ใช้วิธีการหั่นด้วยเครื่องทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลอย่างน้อยตามมาตรฐาน DOD ๕๒๒๐.๒๒ M (การเขียนทับข้อมูลเดิมเป็นจำนวนหลาย ๆ รอบ)
อุปกรณ์สำหรับจัดเก็บที่ไม่สามารถลบข้อมูลได้ เช่น แผ่นซีดีรอมสำหรับอ่านอย่างเดียว	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย

หมายเหตุ : ในกรณีที่ต้องการทำลายข้อมูลในอุปกรณ์สำหรับจัดเก็บนอกเหนือจากตารางข้างต้น ให้แจ้งศูนย์สารสนเทศเพื่อการพัฒนาชุมชนเพื่อขอคำแนะนำในการทำลายข้อมูลที่เหมาะสมเพื่อให้มั่นใจได้ว่าข้อมูลถูกเขียนทับจนไม่สามารถกู้คืนข้อมูลเดิมได้อีก

ภาคผนวก ข.

พระราชกฤษฎีกา
กำหนดหลักเกณฑ์และวิธีการ
ในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ
พ.ศ. ๒๕๔๙

พระราชกฤษฎีกา

กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

พ.ศ. ๒๕๔๙

ภูมิพลอดุลยเดช ป.ร.

ให้ไว้ ณ วันที่ ๒๖ พฤศจิกายน พ.ศ. ๒๕๔๙

เป็นปีที่ ๖๑ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรมินทรมหาภูมิพลอดุลยเดช มีพระบรมราชโองการโปรดเกล้า ฯ ให้ประกาศว่า

โดยที่เป็นการสมควรกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

อาศัยอำนาจตามความในมาตรา ๑๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พุทธศักราช ๒๕๔๙ และมาตรา ๓๕ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ จึงทรงพระกรุณาโปรดเกล้า ฯ ให้ตราพระราชกฤษฎีกาขึ้นไว้ ดังต่อไปนี้

มาตรา ๑ พระราชกฤษฎีกานี้เรียกว่า “พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙”

มาตรา ๒ พระราชกฤษฎีกานี้ให้ใช้บังคับตั้งแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ หน่วยงานของรัฐต้องจัดให้มีระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ในลักษณะ ดังต่อไปนี้

(๑) เอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์นั้นต้องอยู่ในรูปแบบที่เหมาะสม โดยสามารถแสดงหรืออ้างอิงเพื่อใช้ในภายหลังและยังคงความครบถ้วนของข้อความในรูปแบบของข้อมูลอิเล็กทรอนิกส์

(๒) ต้องกำหนดระยะเวลาเริ่มต้นและสิ้นสุดในการยื่นเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ โดยปกติให้ยึดถือวันเวลาของการปฏิบัติงานหน่วยงานของรัฐนั้นเป็นหลัก และอาจกำหนดระยะเวลาในการดำเนินการพิจารณาของหน่วยงานของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ไว้ด้วยก็ได้ เว้นแต่จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

(๓) ต้องกำหนดวิธีการที่ทำให้สามารถระบุตัวเจ้าของลายมือชื่อ ประเภท ลักษณะหรือรูปแบบของลายมือชื่ออิเล็กทรอนิกส์ และสามารถแสดงได้ว่าเจ้าของลายมือชื่อรับรองข้อความในข้อมูลอิเล็กทรอนิกส์

(๔) ต้องกำหนดวิธีการแจ้งการตอบรับด้วยวิธีการทางอิเล็กทรอนิกส์หรือด้วยวิธีการอื่นใดเพื่อเป็นหลักฐานว่าได้มีการดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ไปยังอีกฝ่ายหนึ่งแล้ว

มาตรา ๔ นอกจากที่บัญญัติไว้ในมาตรา ๓ ในกรณีที่หน่วยงานของรัฐจัดทำกระบวนการพิจารณาทางปกครองโดยวิธีการทางอิเล็กทรอนิกส์ ระบบเอกสารที่ทำในรูปของข้อมูลอิเล็กทรอนิกส์ต้องมีลักษณะดังต่อไปนี้ด้วย เว้นแต่จะมีกฎหมายในเรื่องนั้นกำหนดไว้เป็นอย่างอื่น

(๑) มีวิธีการสื่อสารกับผู้ยื่นคำขอในกรณีที่เอกสารมีข้อบกพร่องหรือมีข้อความที่ผิดหลงอันเห็นได้ชัดว่าเกิดจากความไม่รู้หรือความเลินเล่อของผู้ยื่นคำขอ หรือการขอข้อเท็จจริงเพิ่มเติม รวมทั้งมีวิธีการแจ้งสิทธิและหน้าที่ในกระบวนการพิจารณาทางปกครองตามความจำเป็นแก่กรณี ในกรณีที่กฎหมายกำหนดให้ต้องแจ้งให้คู่กรณีทราบ

(๒) ในกรณีมีความจำเป็นตามลักษณะเฉพาะของธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐใด หน่วยงานของรัฐนั้นอาจกำหนดเงื่อนไขว่าคู่กรณียินยอมตกลงและยอมรับการดำเนินการพิจารณาทางปกครองของหน่วยงานของรัฐโดยวิธีการทางอิเล็กทรอนิกส์

มาตรา ๕ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

แนวนโยบายและแนวปฏิบัติอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

มาตรา ๖ ในกรณีที่มีการรวบรวม จัดเก็บ ใช้ หรือเผยแพร่ข้อมูล หรือข้อเท็จจริงที่ทำให้สามารถระบุตัวบุคคล ไม่ว่าโดยตรงหรือโดยอ้อม ให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลด้วย

มาตรา ๗ แนวนโยบายและแนวปฏิบัติตามมาตรา ๕ และมาตรา ๖ ให้หน่วยงานของรัฐจัดทำเป็นประกาศ และต้องได้รับความเห็นชอบจากคณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมาย จึงมีผลใช้บังคับได้

หน่วยงานของรัฐต้องปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่ได้แสดงไว้ และให้จัดให้มีการตรวจสอบการปฏิบัติตามแนวนโยบายและแนวปฏิบัติที่กำหนดไว้อย่างสม่ำเสมอ

มาตรา ๘ ให้คณะกรรมการหรือหน่วยงานที่คณะกรรมการมอบหมายจัดทำแนวนโยบายและแนวปฏิบัติหรือการอื่นอันเกี่ยวกับการดำเนินการตามพระราชกฤษฎีกานี้ ไว้เป็นตัวอย่างเบื้องต้นสำหรับการดำเนินการของหน่วยงานของรัฐในการปฏิบัติตามพระราชกฤษฎีกานี้ และหากหน่วยงานของรัฐแห่งใดมีการปฏิบัติงานตามกฎหมายที่แตกต่างเป็นการเฉพาะแล้ว หน่วยงานของรัฐแห่งนั้นอาจเพิ่มเติมรายละเอียดการปฏิบัติงานตามกฎหมายที่แตกต่างนั้นได้โดยออกเป็นระเบียบ ทั้งนี้ โดยให้คำนึงถึงความถูกต้องครบถ้วน ความน่าเชื่อถือ สภาพความพร้อมใช้งาน และความมั่นคงปลอดภัยของระบบและข้อมูลอิเล็กทรอนิกส์

มาตรา ๙ การทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐตามหลักเกณฑ์และวิธีการตามพระราชกฤษฎีกานี้ ไม่มีผลเป็นการยกเว้นกฎหมายหรือหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนดไว้เพื่อการอนุญาต อนุมัติ การให้ความเห็นชอบ หรือการวินิจฉัย

มาตรา ๑๐ ให้นายกรัฐมนตรีรักษาการตามพระราชกฤษฎีกานี้

ผู้รับสนองพระบรมราชโองการ
พลเอก สุรยุทธ์ จุลานนท์
นายกรัฐมนตรี

หมายเหตุ :- เหตุผลในการประกาศใช้พระราชกฤษฎีกาฉบับนี้ คือ เนื่องจากประเทศไทยได้เริ่มเข้าสู่ยุคสังคมสารสนเทศ ซึ่งมีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐมากขึ้น สมควรสนับสนุนให้หน่วยงานของรัฐมีระบบการบริการของตน โดยการประยุกต์ใช้เทคโนโลยีสารสนเทศเพื่อให้สามารถบริการประชาชนได้อย่างทั่วถึง สะดวก และรวดเร็ว อันเป็นการเพิ่มประสิทธิภาพและประสิทธิผลของหน่วยงานของรัฐ พร้อมกับให้หน่วยงานของรัฐสามารถพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐภายใต้มาตรฐานและเป็นไปในทิศทางเดียวกัน และสร้างความเชื่อมั่นของประชาชนต่อการดำเนินกิจกรรมของรัฐด้วยวิธีการทางอิเล็กทรอนิกส์ ประกอบกับมาตรา ๓๕ วรรคหนึ่ง แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ บัญญัติว่า คำขอ การอนุญาต การจดทะเบียน คำสั่งทางปกครอง การชำระเงิน การประกาศหรือการดำเนินการใด ๆ ตามกฎหมายกับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐ ถ้าได้กระทำในรูปของข้อมูลอิเล็กทรอนิกส์ตามหลักเกณฑ์และวิธีการที่กำหนดโดยพระราชกฤษฎีกาแล้ว ให้ถือว่ามีผลโดยชอบด้วยกฎหมายเช่นเดียวกับการดำเนินการตามหลักเกณฑ์และวิธีการที่กฎหมายในเรื่องนั้นกำหนด จึงจำเป็นต้องตราพระราชกฤษฎีกานี้

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
เรื่อง แนวนโยบายและแนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

พ.ศ. ๒๕๕๓

ด้วยปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับสารสนเทศมีความรุนแรงเพิ่มขึ้นทั้งในประเทศและต่างประเทศ อีกทั้งยังมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้น ทำให้ผู้ประกอบการ ตลอดจนองค์กร ภาครัฐ และภาคเอกชนที่มีการดำเนินงานใด ๆ ในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กร ขาดความเชื่อมั่นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ในทุกรูปแบบ ประกอบกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตระหนักถึงความจำเป็นที่จะส่งเสริมและผลักดันให้ประเทศสามารถยกระดับการแข่งขันกับประเทศอื่น ๆ โดยการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย จึงเห็นความสำคัญที่จะนำกฎหมาย ข้อบังคับต่าง ๆ มาบังคับใช้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ทั้งในส่วนที่ต้องกระทำและในส่วนที่ต้องงดเว้นการกระทำ เพื่อช่วยให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ

เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงได้จัดทำประกาศฉบับนี้ เพื่อเป็นแนวทางเบื้องต้นให้หน่วยงานของรัฐใช้ในการกำหนดนโยบาย และข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ซึ่งอย่างน้อยต้องประกอบด้วยสาระสำคัญ ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

(๑) ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

(๒) สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

(๓) สินทรัพย์ (asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

(๔) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๕) ความมั่นคงปลอดภัยด้านสารสนเทศ (information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

(๖) เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๗) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๒ หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร ซึ่งอย่างน้อยต้องประกอบด้วยเนื้อหา ดังต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๓ หน่วยงานของรัฐต้องจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน ซึ่งอย่างน้อยต้องประกอบด้วยกระบวนการ ดังต่อไปนี้

(๑) หน่วยงานของรัฐต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๒) หน่วยงานของรัฐต้องประกาศนโยบายและข้อปฏิบัติดังกล่าว ให้ผู้เกี่ยวข้องทั้งหมดทราบเพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

(๓) หน่วยงานของรัฐต้องกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติดังกล่าวให้ชัดเจน

(๔) หน่วยงานของรัฐต้องทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอยู่เสมอ

ข้อ ๔ ข้อปฏิบัติในด้านการรักษาความมั่นคงปลอดภัย ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๕ - ๑๕

ข้อ ๕ ให้มีข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) หน่วยงานของรัฐต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงานของรัฐนั้น ๆ

(๓) หน่วยงานของรัฐต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖ ให้มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๗ ให้มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรม หลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๘ ให้มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดข้อปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๙ ให้มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

(๓) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๐ ให้มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑ ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ข้อ ๑๒ หน่วยงานของรัฐที่มีระบบสารสนเทศต้องจัดทำระบบสำรอง ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

(๕) สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

ข้อ ๑๓ หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยต้องมีเนื้อหาอย่างน้อย ดังนี้

(๑) หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ข้อ ๑๔ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจาก

ความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานของรัฐเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๑๕ หน่วยงานของรัฐสามารถเลือกใช้ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่ต่างไปจากประกาศฉบับนี้ได้ หากแสดงให้เห็นว่า ข้อปฏิบัติที่เลือกใช้มีความเหมาะสมกว่า หรือเทียบเท่า

ข้อ ๑๖ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๓๑ พฤษภาคม พ.ศ. ๒๕๕๓
ร้อยตรีหญิง ระนองรักษ์ สุวรรณฉวี
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒)
พ.ศ. ๒๕๕๖

โดยที่เป็นการสมควรปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐให้สอดคล้องกับมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ ๒) พ.ศ. ๒๕๕๖”

ข้อ ๒ ให้ยกเลิกความในข้อ ๑๔ ของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และให้ใช้ความต่อไปนี้แทน

“ข้อ ๑๔ หน่วยงานของรัฐต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น”

ข้อ ๓ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ประกาศ ณ วันที่ ๒๕ มกราคม พ.ศ. ๒๕๕๖
นาวาอากาศเอก อนุดิษฐ์ นาครทรรพ
รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
ประธานกรรมการธุรกรรมทางอิเล็กทรอนิกส์

ที่ปรึกษา

นายนิสิต จันทร์สมวงศ์	อธิบดีกรมการพัฒนาชุมชน
นายทวีป บุตรโพธิ์	รองอธิบดีกรมการพัฒนาชุมชน
นายสมหวัง พ่วงบางโพ	รองอธิบดีกรมการพัฒนาชุมชน
นายโชคชัย แก้วป่อง	รองอธิบดีกรมการพัฒนาชุมชน

คณะผู้จัดทำ

นายชัยยา ขำสะอาด	ผู้อำนวยการศูนย์สารสนเทศเพื่อการพัฒนาชุมชน
นางกาญจนวรรณ ช่วยมั่นคง	ผู้อำนวยการกลุ่มงานระบบสารสนเทศชุมชน
นางสาวทิพพรรณ ไชยูปถัมภ์	ผู้อำนวยการกลุ่มงานข้อมูลพื้นฐานการพัฒนาชนบท
นายอดิศร สุทธิเลิศ	ผู้อำนวยการกลุ่มงานพัฒนาระบบเทคโนโลยีสารสนเทศ
นายชาคริต ถิระสาโรช	ผู้อำนวยการกลุ่มงานพัฒนาระบบเครือข่าย
นายสุริยา บุญเรืองยศศิริ	ผู้อำนวยการกลุ่มงานประสานแผนและข้อมูล
นางสาวปวีณรัตน์ บุตรวงศ์	นักวิชาการพัฒนาชุมชนชำนาญการ
นายยุทธชัย เครือแก้ว	นักวิชาการคอมพิวเตอร์ชำนาญการ
นางสาวกัญธิชา ปัสวาส	นักวิชาการพัฒนาชุมชนชำนาญการ
นายกฤชณัท เพ็ญภักดิ์	นักวิชาการพัฒนาชุมชนชำนาญการ
ว่าที่ ร.ต.ศรายุทธ พิทูรสกุล	นักวิชาการคอมพิวเตอร์ (พนักงานราชการ)
นายภาคภูมิ บัวตูม	นักวิชาการคอมพิวเตอร์ (พนักงานราชการ)

ผู้ตรวจสอบรูปแบบและเนื้อหา กลุ่มงานพัฒนาระบบเครือข่าย

จัดทำโดย กลุ่มงานพัฒนาระบบเครือข่าย ศูนย์สารสนเทศเพื่อการพัฒนาชุมชน
กรมการพัฒนาชุมชน ชั้น ๕ อาคารรัฐประศาสนภักดี ถนนแจ้งวัฒนะ
แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร
โทร ๐-๒๑๔๑-๖๒๙๕ โทรสาร ๐-๒๑๔๓-๘๙๒๐
www.gn.cdd.go.th