ประกาศกรมสรรพสามิต

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒

เพื่อให้การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสรรพสามิต เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ อธิบดีกรมสรรพสามิตโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ให้ยกเลิกประกาศกรมสรรพสามิต เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐ ลงวันที่ ๓๐ มิถุนายน พ.ศ. ๒๕๖๐

ข้อ ๒ ในประกาศนี้

"ผู้ใช้งาน" หมายถึง ข้าราชการ ลูกจ้างประจำ พนักงานราชการ และลูกจ้างชั่วคราว สังกัดกรมสรรพสามิต ที่ปฏิบัติงานเกี่ยวกับระบบสารสนเทศของกรมสรรพสามิต และบุคคลภายนอกที่เข้ามาใช้บริการระบบสารสนเทศของกรมสรรพสามิต รวมถึงหน่วยงานภายนอก ที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศของกรมสรรพสามิต

"สิทธิของผู้ใช้งาน" หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด เพื่อการเข้าถึง หรือเข้าใช้งานระบบสารสนเทศ และสินทรัพย์ที่เกี่ยวกับระบบสารสนเทศ

"สินทรัพย์" หมายถึง ข้อมูล อุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ต่าง ๆ และทรัพย์สินต่าง ๆ ที่มีไว้เพื่อการปฏิบัติงานทางด้านระบบสารสนเทศของกรมสรรพสามิต

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิเข้าถึงหรือการใช้งานอุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบสารสนเทศของกรมสรรพสามิต ทั้งนี้รวมถึงคุณสมบัติในด้าน ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability) ของระบบสารสนเทศของกรมสรรพสามิต

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบเครือข่าย และระบบสารสนเทศ หรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อน หรืออาจสร้างความเสียหายได้ในที่สุด ซึ่งอาจส่งผล

ให้เกิดการหยุดชะงักต่อกระบวนการ หรือขั้นตอนการปฏิบัติงานทางด้านระบบเครือข่าย และระบบสารสนเทศ ของกรมสรรพสามิต ซึ่งแสดงให้เห็นความเป็นไปได้ที่เกิดจากการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายถึง เหตุบกพร่องหรือเหตุละเมิดด้านความมั่นคงปลอดภัย ซึ่งอาจทำให้ระบบสารสนเทศของกรมสรรพสามิตสูญเสียการปฏิบัติงาน รวมถึงการให้บริการต่าง ๆ แต่เพียงบางส่วนหรือทั้งหมดจากการถูกบุกรุก หรือโจมตีทางช่องโหว่ และความมั่นคงปลอดภัยถูกคุกคามจากภัยคุกคามในรูปแบบต่าง ๆ

"อุปกรณ์คอมพิวเตอร์" หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลอัตโนมัติ

"ระบบเครือข่าย" หมายถึง การติดต่อสื่อสาร หรือการรับ - ส่งข้อมูลระหว่างระบบสารสนเทศภายในกรมสรรพสามิตและหน่วยงานอื่น ๆ ที่เกี่ยวข้องกับกรมสรรพสามิต

"ระบบสารสนเทศ" หมายถึง ข้อมูลของกรมสรรพสามิตที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศของกรมสรรพสามิต และสามารถนำสารสนเทศนั้นมาใช้ในการวางแผน การบริหาร การพัฒนา การควบคุม สนับสนุนในภารกิจของกรมสรรพสามิต รวมทั้งนโยบายหรือแนวปฏิบัติในการใช้อุปกรณ์เหล่านี้

"ผู้ดูแลระบบ" หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศให้มีหน้าที่รับผิดชอบในการเป็นผู้ดูแล บริหารจัดการ และรักษาสินทรัพย์ ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศต่าง ๆ ของกรมสรรพสามิต

"หน่วยงานภายนอก" หมายถึง หน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของกรมสรรพสามิต โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

ข้อ ๓ ให้มีนโยบายการควบคุมการเข้าถึงและควบคุมการใช้อุปกรณ์คอมพิวเตอร์ ระบบปฏิบัติการระบบเครือข่าย ระบบสารสนเทศ รวมทั้งการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและระบบสารสนเทศของกรมสรรพสามิต โดยผู้ใช้งานที่มีการปฏิบัติงานเกี่ยวกับระบบสารสนเทศของกรมสรรพสามิต ต้องได้รับการพิสูจน์ตัวตนการเข้าใช้งานก่อนทุกครั้ง และผู้ใช้งานต้องได้รับการพิจารณาอนุมัติตามขั้นตอนที่ระบุไว้อย่างเคร่งครัด และต้องมีการจำกัดสิทธิการเข้าถึงระบบของผู้ใช้งานให้อยู่ในระดับที่เหมาะสมต่อความจำเป็นในการทำงานตามอำนาจหน้าที่ เพื่อให้เกิดความเชื่อมั่นและป้องกันความเสียหายอันเกิดจากการกระทำที่ไม่ถูกต้อง และได้รับสิทธิในการเข้าถึงระบบตามอำนาจหน้าที่ความรับผิดชอบเท่านั้น โดยให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสรรพสามิตท้ายประกาศนี้

ข้อ ๔ ผู้ดูแลระบบต้องจัดให้มีการควบคุมการเข้าถึงระบบสารสนเทศของกรมสรรพสามิต โดยกำหนดให้ผู้ใช้งานต้องได้รับการพิสูจน์ตัวตนของผู้ใช้งานก่อนทุกครั้ง และผู้ใช้งานต้องได้รับพิจารณาอนุญาตให้ใช้งานระบบสารสนเทศเท่าที่จำเป็น ครอบคลุมในทุกขั้นตอน ตั้งแต่การกำหนดวิธีการลงทะเบียนผู้ใช้งาน การบริหารจัดการรหัสผ่านผู้ใช้งานการบริหารจัดการสิทธิการใช้งานระบบสารสนเทศ ให้มีความมั่นคงปลอดภัย และกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงระบบสารสนเทศ ประเภทข้อมูล ลำดับความสำคัญ และการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

ข้อ ๕ ผู้ดูแลระบบต้องบริหารจัดการอุปกรณ์คอมพิวเตอร์ของกรมสรรพสามิตทั้งหมด บริหารจัดการการเข้าถึงและเข้าใช้อุปกรณ์คอมพิวเตอร์ ควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์ ป้องกันอุปกรณ์คอมพิวเตอร์ที่ไม่มีผู้ปฏิบัติงานดูแล กำหนดมาตรการทำลายสื่อบันทึกข้อมูล และข้อมูลอิเล็กทรอนิกส์ กำหนดมาตรการควบคุมการเข้า - ออกห้องควบคุมระบบคอมพิวเตอร์แม่ข่าย บริหารจัดการการเข้าถึงเครือข่าย ควบคุมป้องกันไม่ให้บุคคลที่ไม่มีอำนาจที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึงระบบเครือข่ายที่จะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของกรมสรรพสามิตได้ โดยมีการกำหนดกระบวนการควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่าย บริหารจัดการการเข้าถึงระบบสารสนเทศ กำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากโปรแกรมชุดคำสั่งที่ไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศให้หยุดชะงัก และสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของกรมสรรพสามิตได้

ข้อ ๖ ผู้ใช้งานต้องตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศและต้องปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสรรพสามิตท้ายประกาศนี้อย่างเคร่งครัด โดยต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์ หรือเข้าถึงระบบสารสนเทศของกรมสรรพสามิต และต้องเข้าใจถึงสิทธิการเข้าถึงระบบของผู้ใช้งานต่อความจำเป็นในการทำงานตามอำนาจหน้าที่ความรับผิดชอบสำหรับผู้ใช้งานเองเท่านั้น

ข้อ ๗ ให้มีนโยบายระบบสำรองข้อมูลสารสนเทศและแผนเตรียมความพร้อมกรณีฉุกเฉิน เพื่อให้ผู้ดูแลระบบ สามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบสารสนเทศได้อย่างทันท่วงที รวมทั้งจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของกรมสรรพสามิตบริการได้อย่างต่อเนื่อง รวมทั้งปรับปรุงแก้ไขให้ทันสมัยอยู่เสมอ โดยให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสรรพสามิตท้ายประกาศนี้

ข้อ ๘ ให้มีนโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศของกรมสรรพสามิต โดยให้เป็นไปตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสรรพสามิตท้ายประกาศนี้

ข้อ ๙ ให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่ดูแล บริหารจัดการ และรักษาสินทรัพย์ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศต่าง ๆ ของกรมสรรพสามิต พร้อมทั้งแต่งตั้งผู้ดูแลระบบให้มีหน้าที่รับผิดชอบในการเป็นผู้ดูแล บริหารจัดการ และรักษาสินทรัพย์ ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศต่าง ๆ ของกรมสรรพสามิต ให้สอดคล้องตามนโยบายนี้

ข้อ ๑๐ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสรรพสามิตและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสรรพสามิตท้ายประกาศนี้ ให้มีการทบทวนปรับปรุงให้มีความทันสมัยอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อระบบสารสนเทศมีการเปลี่ยนแปลงที่สำคัญ

ข้อ ๑๑ กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่กรมสรรพสามิต หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ให้อธิบดีกรมสรรพสามิตเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๑๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๑๑ มิถุนายน พ.ศ. ๒๕๖๒

(นายพชร อนันตศิลป์)
อธิบดีกรมสรรพสามิต

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสรรพสามิต

สารบัญ

๑. แนวปฏิบัติการควบคุมการเข้าถึงและควบคุมการใช้อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ

เพื่อกำหนดเป็นมาตรการ มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้อง เข้าถึงและใช้อุปกรณ์คอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ของกรมสรรพสามิต โดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการเข้าถึง เพื่อให้สามารถตรวจสอบ ติดตาม พิสูจน์ตัวบุคคลได้ โดยมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศ และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ โดยมีแนวทางการปฏิบัติ ดังนี้

๑.๑ การควบคุมการเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ (Access Control)

๑.๑.๑ จัดทำบัญชีสินทรัพย์หรือทะเบียนสินทรัพย์ การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

(๑) การบริหารจัดการสินทรัพย์ โดยผู้ดูแลระบบ ทำการส่งข้อมูลรายละเอียดรายการสินทรัพย์ที่ต้องการขึ้นทะเบียนใหม่ ให้เจ้าหน้าที่ส่วนบริหารการพัสดุ เพื่อร้องขอให้ออกหมายเลขครุภัณฑ์

(๒) เจ้าหน้าที่ส่วนบริหารการพัสดุ ส่งหมายเลขดังกล่าวให้กับผู้ดูแลระบบดำเนินการบันทึกข้อมูลในแบบฟอร์มบันทึกรายการสินทรัพย์ และให้ผู้ดูแลระบบดำเนินการติดป้ายหมายเลขครุภัณฑ์

(๓) การจัดจำหน่ายทรัพย์สิน โดยผู้ดูแลระบบ ทำการสำรวจรายการสินทรัพย์ ของศูนย์เทคโนโลยีสารสนเทศตามรอบที่กำหนดให้แก่ผู้อนุมัติ เพื่อให้ผู้อนุมัติพิจารณาสินทรัพย์ ที่ต้องการจัดจำหน่าย ดำเนินการบันทึกการตรวจสอบ และแจ้งกลับผู้ดูแลระบบ เพื่อสรุปผลการสำรวจรายการสินทรัพย์ที่ต้องจัดจำหน่ายทั้งหมดและนำเสนอต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อพิจารณาต่อไป

๑.๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึง และควบคุมการใช้งานระบบสารสนเทศ โดยกำหนดให้มีการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น อ่านอย่างเดียว สร้างข้อมูล ป้อนข้อมูล แก้ไข อนุมัติ ไม่มีสิทธิ เป็นต้น

(๒) กำหนดเกณฑ์การระงับสิทธิ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการใช้งานระบบสารสนเทศของกรมสรรพสามิต จะต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูล ได้แก่

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี

- ข้อมูลสารสนเทศด้านภาษีสรรพสามิตที่ให้บริการ ได้แก่ ข้อมูลผู้ประกอบอุตสาหกรรม ข้อมูลรายได้ ข้อมูลการปราบปรามผู้กระทำผิดเกี่ยวกับกฎหมายสรรพสามิต ข้อมูลส่วนบุคคล

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ ได้แก่

- ข้อมูลสารสนเทศที่มีระดับความสำคัญมากที่สุด
- ข้อมูลสารสนเทศที่มีระดับความสำคัญปานกลาง
- ข้อมูลสารสนเทศที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล ได้แก่

- ลับที่สุด (Top Secret) หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญมากที่สุดต่อการดำเนินงานของกรมสรรพสามิต และกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือใช้สารสนเทศดังกล่าวได้ การเปิดเผยทั้งหมดหรือบางส่วน หรือการเข้าถึงสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาต จะเกิดความเสียหายแก่ประโยชน์แห่งรัฐหรือกรมสรรพสามิตอย่างร้ายแรงที่สุด

- ลับมาก (Secret) หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญปานกลางต่อการดำเนินงานของกรมสรรพสามิต และกำหนดให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น ที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ การเปิดเผยทั้งหมดหรือเพียงบางส่วน หรือการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาต จะเกิดความเสียหายแก่ประโยชน์แห่งรัฐหรือกรมสรรพสามิตอย่างร้ายแรง

- ลับ (Confidential) หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญปานกลางต่อการดำเนินงานของกรมสรรพสามิต และกำหนดให้บุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือใช้ข้อมูลสารสนเทศดังกล่าวได้ การเปิดเผยหรือการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้โดยไม่ได้รับอนุญาต จะเกิดความเสียหายแก่ประโยชน์แห่งรัฐหรือกรมสรรพสามิต

- ใช้ภายใน (Internal Use) หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญต่ำต่อการดำเนินงานธุรกิจของกรมสรรพสามิต สารสนเทศลำดับชั้นใช้ภายในนี้ จะอนุญาตให้ใช้ภายในหน่วยงานที่กำหนดเท่านั้น การเปิดเผยหรือการเข้าถึงข้อมูลสารสนเทศในระดับชั้นนี้ โดยไม่ได้รับอนุญาตอาจก่อให้เกิดผลกระทบต่อการปฏิบัติงานประจำวันของหน่วยงานดังกล่าว แต่ไม่กระทบต่อการดำเนินงาน หรือเกิดความเสียหายแก่ประโยชน์แห่งรัฐหรือกรมสรรพสามิต

- ทั่วไป (Public) หมายถึง ข้อมูลสารสนเทศที่มีระดับความสำคัญต่ำต่อการดำเนินงานของกรมสรรพสามิต สารสนเทศลำดับชั้นทั่วไปนี้ เป็นข้อมูลสารสนเทศที่ผู้บริหารอนุมัติให้เปิดเผยต่อสาธารณะได้ อย่างไรก็ดี ข้อมูลสารสนเทศในระดับชั้นนี้ต้องได้รับการป้องกัน หรือควบคุมอย่างเหมาะสม เพื่อให้มั่นใจว่าข้อมูลสารสนเทศที่ถูกเปิดเผยมีความถูกต้องครบถ้วน (Integrity) เพื่อสร้างความเชื่อมั่นให้แก่ผู้ใช้งานสารสนเทศรวมทั้งรักษาภาพลักษณ์และชื่อเสียงของกรมสรรพสามิต

(๔) จัดแบ่งระดับชั้นการเข้าถึง ได้แก่

- ระดับชั้นสำหรับผู้บริหาร คือ ข้าราชการกรมสรรพสามิต ระดับผู้อำนวยการสำนักขึ้นไป ที่มีหน้าที่เกี่ยวข้องและต้องได้รับอนุญาตจากผู้บังคับบัญชา ระดับรองอธิบดีหรือเทียบเท่าขึ้นไป

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป คือ ข้าราชการกรมสรรพสามิต ที่มีหน้าที่เกี่ยวข้องและต้องได้รับอนุญาตจากผู้บังคับบัญชา ระดับผู้อำนวยการสำนักหรือเทียบเท่าขึ้นไป

- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย คือ ข้าราชการกรมสรรพสามิต ที่มีหน้าที่เกี่ยวข้อง และต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๕) การกำหนดเวลาที่ได้เข้าถึง

- การเข้าถึงระบบสารสนเทศในเวลาราชการ (๐๘.๓๐ – ๑๖.๓๐ น.)

- การเข้าถึงระบบสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา ๐๘.๓๐ - ๑๖.๓๐ น.)

- การเข้าถึงระบบสารสนเทศในช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนักขัตฤกษ์)

- การเข้าถึงระบบสารสนเทศในช่วงเวลาพิเศษเป็นรายครั้ง ต้องระบุช่วงเวลาและจำนวนระยะเวลาการเข้าถึง ทั้งนี้ ระยะเวลาการเข้าถึง ได้แก่ ๑ วัน ๑ ถึง ๓ วัน ๑ สัปดาห์ ๑ เดือน ๓ เดือน ๑ ปีงบประมาณ หรือตามเวลาที่ร้องขอ

(๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

- ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)

- เคาน์เตอร์บริการ (เข้าถึงได้ในเวลาราชการ)

- โทรศัพท์หรือโทรสาร (เข้าถึงได้ในเวลาราชการ)

- หนังสือหรือบันทึกข้อความ (เข้าถึงได้ในเวลาราชการ)

- ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

- ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

- ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

- เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา)

- การประชุมทางไกล (เข้าถึงได้ในเวลาราชการ และในช่วงเวลาพิเศษเป็นรายครั้ง)

๑.๑.๔ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑) มีการควบคุมการเข้าถึงระบบสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศให้สามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตแล้ว และสร้างความรู้ความเข้าใจให้กับผู้ใช้งานด้านการจัดการโดยการจัดฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ให้ปฏิบัติ ดังนี้

๑.๒.๑ มีการกำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) อย่างน้อยปีละ ๑ ครั้ง

๑.๒.๒ ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๑.๒.๓ การลงทะเบียนและการระงับสิทธิผู้ใช้งาน (User Registration and De-Registration)

(๑) การลงทะเบียนผู้ใช้งานในระบบสารสนเทศ ให้ผู้ร้องขอ กรอกแบบฟอร์มการลงทะเบียนผู้ใช้งาน ให้ผู้อนุมัติพิจารณาความเหมาะสมของระดับสิทธิที่ร้องขอ เจ้าหน้าที่ผู้ดูแลระบบกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) จัดส่งให้กับผู้ร้องขอ

(๒) การแก้ไขเปลี่ยนแปลงสิทธิผู้ใช้งานในระบบสารสนเทศ ให้ผู้ร้องขอ กรอกแบบฟอร์มการลงทะเบียนผู้ใช้งานให้ผู้อนุมัติพิจารณาความเหมาะสมของการแก้ไขเปลี่ยนแปลงสิทธิ จากนั้นให้เจ้าหน้าที่ผู้ดูแลระบบดำเนินการแก้ไขเปลี่ยนแปลงสิทธิผู้ใช้งาน

(๓) การระงับสิทธิผู้ใช้งานในระบบสารสนเทศ ให้ผู้ร้องขอ กรอกแบบฟอร์มการลงทะเบียนผู้ใช้งานให้ผู้อนุมัติพิจารณาการระงับสิทธิ จากนั้นให้เจ้าหน้าที่ผู้ดูแลระบบดำเนินการระงับสิทธิผู้ใช้งาน

(๔) ต้องกำหนดให้มีการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งานในการเข้าถึงข้อมูลหรือระบบสารสนเทศตามหน้าที่ความรับผิดชอบ

(๕) ต้องจัดทำเอกสารการมอบหมายสิทธิการเข้าถึงข้อมูลหรือระบบสารสนเทศ และจัดเก็บไว้เป็นหลักฐานในการดำเนินงาน

๑.๒.๔ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

(๒) การกำหนดชื่อผู้ใช้งาน (User Name) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำ ให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานอื่น

(๓) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

(๔) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ โดยให้ผู้ร้องขอ กรอกแบบฟอร์มการลงทะเบียนผู้ใช้งานให้ผู้อนุมัติพิจารณาความเหมาะสมในการขอใช้งานสิทธิผู้ดูแลระบบระดับสูงสุด จากนั้นให้เจ้าหน้าที่ผู้ดูแลระบบ จัดส่งชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ให้กับผู้ร้องขอ เมื่อใช้งานเสร็จสิ้นให้ดำเนินการส่งคืนรหัสผ่านให้กับผู้ดูแลระบบ จากนั้นผู้ดูแลระบบต้องดำเนินการเปลี่ยนรหัสผ่านใหม่และจัดเก็บซองรหัสผ่านในตู้ที่มีการปิดล็อกอย่างมั่นคงปลอดภัย

๑.๒.๕ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ให้ผู้ดูแลระบบจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) ต้องมีการเปลี่ยนรหัสผ่านอัตโนมัติทุก ๆ ๖ เดือน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน หรือทันทีที่ได้รับสัญญาณบอกเหตุว่ารหัสผ่านอาจรั่วไหล

(๒) จำนวนตัวอักษรมากกว่าหรือเท่ากับ ๘ ตัวอักษร

(๓) ต้องมีการผสมกันระหว่างตัวอักษรอักขระอย่างน้อย ๓ ประเภท ดังนี้

- ตัวเลข (Numerical Character)
- ตัวอักษร (Alphabet)
- ตัวอักขระพิเศษ (Special Character)

(๔) ไม่ตั้งรหัสผ่านด้วย ชื่อ วันเดือนปีเกิด หรือข้อความใดที่ง่ายต่อการล่วงรู้หรือง่ายต่อการคาดเดา

(๕) กำหนดให้ระบบปฏิบัติการ Microsoft Windows และ อุปกรณ์เครือข่าย ไม่ใช้งานรหัสผ่านซึ่งเคยใช้มาแล้ว (Password History) อย่างน้อย ๕ รหัสผ่านที่เคยใช้งานล่าสุด

(๖) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ห้ามใช้บุคคลอื่นในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(๗) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน และผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

(๘) เปลี่ยนรหัสผ่านตั้งต้นของระบบสารสนเทศทันทีหลังจากติดตั้งระบบสารสนเทศใหม่

(๙) การเปลี่ยนรหัสผ่าน ต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๑๐) กำหนดให้ระบบสารสนเทศแสดงเฉพาะข้อมูลที่จำเป็นในการล็อกอินเท่านั้น ไม่ควรแสดงข้อมูลของระบบ เช่น ประเภทของอุปกรณ์ เวอร์ชันของซอฟต์แวร์ หรือข้อมูลใด ๆ ที่แสดงให้เห็นถึงรายละเอียดของระบบ เป็นต้น

(๑๑) กำหนดให้ระบบสารสนเทศไม่แสดงระบบให้ความช่วยเหลือใด ๆ เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีสามารถใช้ประโยชน์จากข้อมูลช่วยเหลือ

(๑๒) กำหนดให้ระบบสารสนเทศใช้สัญลักษณ์ใด ๆ แทนการแสดงรหัสผ่านในช่องใส่รหัสผ่านระหว่างที่ผู้ใช้กำลังใส่ข้อมูลล็อกอิน เช่น เครื่องหมายจุด เครื่องหมายสี่เหลี่ยม หรือเครื่องหมายดอกจัน เป็นต้น

(๑๓) กำหนดให้ระบบสารสนเทศจำกัดจำนวนครั้งที่ผู้ใช้งานสามารถใส่ข้อมูลการล็อกอินผิด เช่น ไม่เกิน ๓ ครั้ง เป็นต้น และกำหนดให้ผู้ใช้งานไม่สามารถล็อกอินได้หลังจากที่ล็อกอินผิดตามจำนวนที่กำหนดไว้

(๑๔) กำหนดให้ระบบสารสนเทศมีการเข้ารหัสลับข้อมูลการล็อกอินในการส่งผ่านเครือข่ายและในส่วนที่จัดเก็บข้อมูลรหัสผ่าน

(๑๕) กำหนดให้ระบบสารสนเทศมีการเก็บข้อมูลการล็อกอินสำเร็จ และไม่สำเร็จ

(๑๖) กำหนดช่วงระยะเวลานานที่สุด (Session timeout) ที่ผู้ใช้งานจะสามารถเข้าใช้ระบบสารสนเทศให้สำเร็จ

(๑๗) จำกัดเวลาการเชื่อมต่อสำหรับระบบสารสนเทศที่มีความเสี่ยงสูง หรือระบบสารสนเทศที่มีความสำคัญ เพื่อลดโอกาสในการเข้าถึงโดยไม่ได้รับอนุญาต

๑.๒.๖ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น เพื่อให้มั่นใจว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม โดยผู้ดูแลระบบ ดำเนินการรวบรวมรายการสิทธิของผู้ใช้งานในระบบต่าง ๆ และบันทึกลงในแบบฟอร์มการดำเนินการทบทวนสิทธิ เพื่อส่งให้ผู้ใช้งาน หรือหน่วยงานต้นสังกัดของผู้ใช้งาน พิจารณาทบทวนความเหมาะสมของสิทธิการเข้าถึงระบบสารสนเทศในปัจจุบัน โดยหากต้องการปรับปรุงแก้ไขสิทธิ ให้แจ้งผู้ดูแลระบบเพื่อดำเนินการปรับปรุงแก้ไขสิทธิ ตามผลการทบทวน

๑.๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ ให้ปฏิบัติ ดังนี้

๑.๓.๑ การกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

(๑) ผู้ดูแลระบบต้องมีการบริหารจัดการรหัสผ่าน โดยให้ระบบคอมพิวเตอร์กำหนดการสร้างรหัสผ่านชั่วคราวให้อัตโนมัติ และเมื่อส่งให้ผู้ใช้งาน ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ควรตั้งรหัสผ่านที่ยากต่อการคาดเดา และให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๓) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเอง หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๔) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๕) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๖) เก็บรักษารหัสผ่านไว้เป็นความลับ

(๗) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๘) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(๙) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๐) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๑) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๒) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบสารสนเทศต่าง ๆ ที่ตนใช้งาน

(๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๔) ผู้ดูแลระบบต้องเปลี่ยนรหัสถี่กว่าผู้ใช้งานทั่วไป

๑.๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ สามารถเข้าถึงอุปกรณ์ของกรมสรรพสามิต ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๒) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

๑.๓.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(๑) ผู้ดูแลระบบ ต้องกำหนดมาตรการป้องกันสินทรัพย์ขององค์กรให้ครอบคลุมเรื่องต่าง ๆ โดยควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น การจัดการบริเวณล้อมรอบ การควบคุมการเข้า-ออก การจัดบริเวณการเข้าถึง การส่งผลิตภัณฑ์โดยบุคคลภายนอก การวางอุปกรณ์ ระบบและอุปกรณ์สนับสนุนการทำงาน เป็นต้น

(๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่าง ๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ
- วัฒนธรรมองค์กร

(๓) ผู้ดูแลระบบ ต้องกำหนดให้มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน และต้องกำหนดให้ผู้ใช้งาน ออกจากระบบโดยทันทีเมื่อเสร็จสิ้นงาน

(๔) มีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ผู้ใช้งานต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันสินทรัพย์ของกรมสรรพสามิต
- ผู้ใช้งานต้องลงชื่อออกจากระบบทันที เมื่อไม่ได้ใช้งาน หรือจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต เช่น กล้องดิจิตอล โทรศัพท์มือถือ เครื่องถ่ายเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

(๕) มีมาตรการทำลายสื่อบันทึกข้อมูล และข้อมูลอิเล็กทรอนิกส์ ดังนี้

- ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรืออุปกรณ์บันทึกข้อมูลอื่น โดยการฟอร์แมตอุปกรณ์ดังกล่าวให้ไม่สามารถเรียกข้อมูลกลับมาได้ ก่อนทำการเปลี่ยน ทดแทน ทำลาย หรือจำหน่าย

- ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติในการทำลายอุปกรณ์บันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

๑.๓.๔ การจัดหาและการพัฒนาระบบสารสนเทศใหม่ หรือการปรับปรุงจากระบบที่มีอยู่เดิม ต้องมีการวิเคราะห์และระบุข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศไว้ด้วย โดยนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

(๑) ต้องมีระบบล็อกอินเข้าใช้งานระบบสารสนเทศ และต้องมีการกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ

(๒) ต้องมีระบบป้องกันการรักษาความปลอดภัยของข้อมูลสารสนเทศให้กับระบบสารสนเทศที่เป็นแบบเว็บแอพพลิเคชั่นโดยใช้การเข้ารหัสข้อมูลผ่านโปรโตคอล Secure Sockets Layer (SSL)

๑.๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ให้ผู้ดูแลระบบปฏิบัติ ดังนี้

๑.๔.๑ การใช้บริการเครือข่าย ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของการให้บริการ ได้แก่ โซนภายใน (Internal Zone) และ โซนภายนอก (External Zone) เพื่อควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ และต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) ผู้ดูแลระบบต้องกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้มีการใช้งานได้

(๒) มีข้อปฏิบัติสำหรับผู้ใช้งาน ให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น พร้อมทั้งจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย ก่อนที่จะใช้งานในทุกกรณี

(๓) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยผู้ดูแลระบบต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๑.๔.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

(๑) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน จะต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศก่อนทุกครั้ง และมีการควบคุมอย่างเข้มงวด โดยผู้ใช้งานจะต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการขออนุญาต อย่างเพียงพอ

(๒) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (User Name) ทุกครั้ง และผู้ดูแลระบบจะต้องตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของกรมสรรพสามิต อย่างน้อย ๑ วิธี เช่น มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม เป็นต้น

(๓) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศของกรมสรรพสามิต โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

(๔) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตที่ใช้ไว้ตลอดเวลาโดยไม่จำเป็น ควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๑.๔.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ผู้ดูและระบบต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๑) การควบคุมการใช้งานอย่างเหมาะสม และจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้โดยผู้ขอใช้บริการ จะต้องได้รับการอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศก่อนทุกครั้ง

(๒) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์ โดยผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย เช่น รายชื่อผู้ขอใช้บริการ IP Address Mac Address และผังเครือข่าย เป็นต้น

(๓) อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของต้นทางและปลายทางได้

๑.๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย ดังนี้

(๑) ผู้ดูแลระบบ ต้องกำหนดการเปิด - ปิด พอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงของอุปกรณ์เครือข่ายต่าง ๆ และปิดพอร์ตที่เสี่ยงต่อการก่อให้เกิดความเสียหายต่อระบบเครือข่ายและอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๒) บุคคลภายนอกที่เข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายต้องได้รับการอนุญาตจากผู้ดูแลระบบ

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๑.๔.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายภายในหน่วยงาน และเครือข่ายภายนอกหน่วยงาน

๑.๔.๖ การควบคุมการเชื่อมต่อเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกัน ดังนี้

(๑) ผู้ดูแลระบบต้องมีการตรวจสอบการเชื่อมต่อเครือข่าย

(๒) จำกัดสิทธิของผู้ใช้ในการเชื่อมต่อเครือข่าย

(๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(๔) ผู้ดูแลระบบต้องมีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ผู้ดูแลระบบต้องควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๑.๔.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลสารสนเทศ ดังนี้

(๑) ควบคุมไม่ให้มีการเปิดเผยการใช้หมายเลขเครือข่าย (IP Address)

(๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมต่อเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๑.๔.๘ การควบคุมการเข้าใช้งานระบบจากระยะไกล (Remote Access)

(๑) ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) ต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

(๓) ผู้ใช้งานต้องแสดงหลักฐานและเหตุผลความจำเป็น และต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๔) มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม ต้องดูแลและจัดการโดยผู้ดูแลระบบ และต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๑.๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาตให้ปฏิบัติ ดังนี้

๑.๕.๑ ผู้ดูแลระบบ (System Administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของกรมสรรพสามิตและกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) ให้กับผู้ใช้งานเพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของกรมสรรพสามิต

๑.๕.๒ การเข้าใช้งานและการเข้าถึงระบบปฏิบัติการ

(๑) ผู้ดูแลระบบ ต้องจัดไม่ให้ระบบปฏิบัติการแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบปฏิบัติการก่อนที่การเข้าสู่ระบบปฏิบัติการจะเสร็จสมบูรณ์

(๒) ระบบปฏิบัติการต้องสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๓) ต้องจำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line

๑.๕.๓ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง ดังนี้

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของกรมสรรพสามิต ให้เป็นไปตามการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน ใน ข้อที่ ๑.๓.๑

(๒) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น Smart Card เป็นต้น

๑.๕.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิด สามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ หรือที่มีอยู่แล้ว โดยให้ผู้ดูแลระบบดำเนินการ ดังนี้

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์ ห้ามลงโปรแกรมที่ไม่ได้รับอนุญาต ห้ามลงโปรแกรมที่ละเมิดลิขสิทธิ์

(๒) ให้ผู้ดูแลระบบตรวจสอบโปรแกรมอรรถประโยชน์ และต้องได้รับการอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย ก่อนการใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๑.๕.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง ให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out) เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๑) กรณีระบบสารสนเทศทั่วไป ให้ยุติการใช้งานเมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาที

(๒) กรณีระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญสูง ให้ยุติการใช้งานเมื่อว่างเว้นจากการใช้งานเป็นเวลา ๑๕ นาที

๑.๕.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทาง และต้องจำกัดระยะเวลาในการเชื่อมต่อ เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น โดยกำหนดให้ใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง หรือกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของกรมสรรพสามิตตามปกติ เป็นต้น

๑.๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

ผู้ดูแลระบบต้องมีการควบคุม อย่างน้อยดังนี้

๑.๖.๑ การจำกัดการเข้าถึงระบบสารสนเทศ (Information Access Restriction) ผู้ดูแลระบบต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึง

ระบบสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยเป็นไปตามหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึง หรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงระบบสารสนเทศที่ได้กำหนดไว้

๑.๖.๒ ระบบสารสนเทศซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อกรมสรรพสามิต ผู้ดูแลระบบต้องมีการควบคุมและให้ดำเนินการ ดังนี้

(๑) แยกระบบสารสนเทศซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อกรมสรรพสามิต ได้แก่

- ระบบงานทะเบียนสรรพสามิต
- ระบบงานการขอใบอนุญาต
- ระบบงานรายได้
- ระบบขอยกเว้นภาษี คืนภาษี และลดหย่อนภาษี
- ระบบวิเคราะห์รายการภาษี
- ระบบงานฐานข้อมูลอ้างอิงกลาง

(๒) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวใน (๑) โดยเฉพาะ

(๓) มีการควบคุมอุปกรณ์คอมพิวเตอร์ ระบบสื่อสารและการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าวใน (๑)

๑.๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่ ผู้ดูแลระบบต้องมีการกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่เพื่อปกป้องข้อมูลสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่ และต้องไม่ให้บุคคลภายนอกคัดลอกข้อมูลสารสนเทศจากอุปกรณ์คอมพิวเตอร์ที่นำไปใช้ได้ มีการเก็บข้อมูลเกี่ยวกับอุปกรณ์คอมพิวเตอร์เคลื่อนที่ ชื่อผู้ใช้งาน ซึ่งหากปรากฏความเสียหายร้ายแรง ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น นอกจากนี้ ผู้ใช้งาน ต้องปฏิบัติ ดังนี้

(๑) เครื่องคอมพิวเตอร์ที่กรมสรรพสามิตมอบให้ผู้ใช้งาน เป็นทรัพย์สินของกรมสรรพสามิต ดังนั้น ผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของกรมสรรพสามิต เท่านั้น

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของกรมสรรพสามิต ต้องเป็นโปรแกรมที่กรมสรรพสามิตได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือนำไปให้ผู้อื่นใช้งาน

(๓) ผู้ใช้งาน มีหน้าที่ดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ และต้องรับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นนั้นด้วย

(๔) ปิดเครื่องคอมพิวเตอร์เมื่อไม่ใช้งานหรือเสร็จสิ้นการใช้งานแล้วในทันที

(๕) ทำการล็อคหน้าจอเครื่องคอมพิวเตอร์หลังจากที่ไม่ได้ใช้งานเป็นเวลา ๕ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

(๖) การนำเครื่องคอมพิวเตอร์มาใช้กับระบบเครือข่ายของกรมสรรพสามิต ต้องพิสูจน์ตัวตนผ่านระบบพิสูจน์ตัวตนก่อนเข้าใช้งานทุกครั้ง

(๗) ไม่อนุญาตให้เข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม

(๘) ห้ามผู้ใช้งานใช้อุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่กระทำความผิด ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

๑.๖.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน ผู้ดูแลระบบต้องกำหนดขั้นตอนการขออนุมัติการปฏิบัติงานจากภายนอกหน่วยงาน กำหนดสิทธิหรือระงับสิทธิการเข้าถึงระบบสารสนเทศ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งในการปฏิบัติงานจากภายนอกหน่วยงาน หากปรากฏความเสียหายร้ายแรง ผู้ปฏิบัติงานจากภายนอกหน่วยงานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น นอกจากนี้ ผู้ใช้งาน ต้องปฏิบัติ ดังนี้

(๑) กรอกแบบฟอร์มการขอใช้งานจากภายนอก

(๒) ชี้แจงแผนงานและขั้นตอนปฏิบัติ เพื่อเสนอการขออนุมัติการขอใช้งานจากภายนอก

(๓) ตรวจสอบการทำงานอย่างเคร่งครัด

๑.๖.๕ ในกรณีที่กรมสรรพสามิตได้มีการว่าจ้างกับบริษัทต่าง ๆ เพื่อดำเนินโครงการของการพัฒนาระบบสารสนเทศ ของกรมสรรพสามิต และต้องลงนามในสัญญาการว่าจ้างกับบริษัทต่าง ๆ ให้มีการจัดทำเอกสารแนบท้ายสัญญาว่าด้วยการรักษาข้อมูลที่เป็นความลับด้านระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลสารสนเทศ ของกรมสรรพสามิต กับบริษัทคู่สัญญา โดยมีการกำหนดมาตรการ ดังนี้

(๑) ผู้รับจ้างมีหน้าที่ในการคัดสรรพนักงานที่เข้ามาดำเนินโครงการของการพัฒนาระบบสารสนเทศของกรมสรรพสามิต จะต้องไม่เคยเป็นผู้มีความผิดเกี่ยวกับการกระทำความผิดทางคอมพิวเตอร์ ระหว่างการจ้างผู้รับจ้างมีหน้าที่และความรับผิดชอบในการควบคุมดูแลพนักงานของผู้รับจ้างให้รักษาข้อมูลที่เป็นความลับเช่นเดียวกับที่ผู้รับจ้างต้องปฏิบัติ ผู้รับจ้างจะต้องใช้ความระมัดระวังอย่างที่สุดตามที่ผู้ประกอบวิชาชีพจะพึงมีในการรักษาข้อมูลที่เป็นความลับอย่างเคร่งครัด โดยไม่บอกหรือเปิดเผยข้อมูลที่เป็นความลับแก่บุคคลภายนอกรู้ ไม่ว่ากรณีใด ๆ ทั้งสิ้น เว้นแต่เพื่อความจำเป็นในการปฏิบัติงานตามหน้าที่ของผู้รับจ้างตามสัญญาหลักเท่านั้น ต้องเสริมสร้างความเข้าใจอันดีต่อพนักงานทุกคน เพื่อให้การปฏิบัติและการบริหารงานด้านการรักษาข้อมูลบังเกิดผลมากที่สุด

(๒) เมื่อสิ้นสุดการปฏิบัติงานตามสัญญาหลักหรือสัญญาหลักสิ้นสุดลงไม่ว่าด้วยเหตุใด ๆ ผู้รับจ้างต้องคืนเอกสาร แบบแปลน พิมพ์เขียว หรือคู่มือปฏิบัติงานเกี่ยวกับงานที่ว่าจ้างที่ได้รับไปจากผู้ว่าจ้างทันที และมิให้ทำสำเนาไว้ไม่ว่าในรูปของเอกสารหรือข้อมูลอิเล็กทรอนิกส์อื่นใดทั้งสิ้น

๑.๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๑.๗.๑ ผู้ดูแลระบบ ต้องดำเนินการดังต่อไปนี้

(๑) ทำการลงทะเบียนผู้ใช้งานระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนอนุญาตให้เข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงระบบเครือข่ายไร้สายอย่างสม่ำเสมอ

(๒) ทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้เชื่อมต่อกับระบบเครือข่ายไร้สาย

(๓) ควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๔) ทำการเปลี่ยนค่า SSID (Service Set IDentifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(๕) เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

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

(๗) เลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (User Name) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้ (User Name) รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้

(๘) มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในกรมสรรพสามิต

(๙) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบโดยทันที

๑.๗.๒ ผู้ใช้งานที่จะใช้งานระบบเครือข่ายไร้สายของกรมสรรพสามิต ต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย ผู้ใช้งานมีหน้าที่ระมัดระวังความปลอดภัยในการใช้งานเครือข่ายไร้สาย (Wireless Lan) และต้องใช้งานผ่านบัญชีผู้ใช้ของตนเอง

๑.๗.๓ ผู้ใช้งาน ต้องไม่ดำเนินการดังต่อไปนี้

(๑) นำอุปกรณ์ไร้สาย มาติดตั้งหรือเปิดใช้งานเองในกรมสรรพสามิตไม่ว่าจะเป็น Access Point, Wireless Routers, Wireless USB Client หรือ Wireless Card

(๒) เปิดระบบเครือข่ายไร้สายแบบจุดต่อจุด (Ad-Hoc) หรือ Peer-to-Peer Network

(๓) นำรหัสผ่านที่ได้รับอนุญาตไปทำการเปิดเผยต่อผู้อื่นหรือสาธารณะ

(๔) โอน จำหน่าย หรือจ่ายแจกสิทธิที่ผู้ใช้งานได้รับ ให้กับผู้อื่น

(๕) ให้ผู้อื่นใช้งานผ่านบัญชีผู้ใช้ของตน หากเกิดปัญหาใด ๆ เจ้าของบัญชีจะต้องเป็นผู้รับผิดชอบทุกกรณี

๑.๘ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๑.๘.๑ การรักษาความมั่นคงปลอดภัยของศูนย์คอมพิวเตอร์ (ห้อง Data Center)

(๑) ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ใช้งานระบบสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็น พื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

(๒) ให้ศูนย์เทคโนโลยีสารสนเทศ เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศ

(๓) ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศ

(๓.๑) การเข้า-ออกพื้นที่ห้อง Data Center ในกรณีต้องการนำทรัพย์สินเข้า-ออกห้อง Data Center ผู้ร้องขอต้องกรอกแบบฟอร์มการขอเข้าพื้นที่ห้อง Data Center และนำอุปกรณ์เข้า-ออกให้ผู้ดูแลระบบพิจารณาคำร้องขอ จากนั้นส่งให้เจ้าหน้าที่ส่วนบริหารคอมพิวเตอร์และเครือข่ายพิจารณาอนุมัติ โดยเมื่อเข้าถึงพื้นที่ห้อง Data Center ต้องลงนามในบันทึกการเข้า–ออกพื้นที่ควบคุมทุกครั้ง

(๓.๒) การเข้า-ออกพื้นที่ห้อง Data Center ในกรณีที่มีความประสงค์เข้าถึงพื้นที่ห้อง Data Center เพื่อดำเนินการแก้ไขหรือเปลี่ยนแปลงระบบงาน ผู้ร้องขอต้องกรอกแบบฟอร์มการขออนุญาต แก้ไข/เปลี่ยนแปลง/ติดตั้งระบบงาน/บำรุงรักษาระบบ ให้ผู้ดูแลระบบพิจารณาคำร้องขอ จากนั้นส่งให้เจ้าหน้าที่ส่วนบริหารคอมพิวเตอร์และเครือข่ายพิจารณาอนุมัติ โดยเมื่อเข้าถึงพื้นที่ห้อง Data Center ต้องลงนามในบันทึกการเข้า–ออกพื้นที่ควบคุมทุกครั้ง

(๓.๓) การเข้า-ออกพื้นที่ห้อง Data Center ในกรณีการเข้าพื้นที่ในวันหยุดราชการ ผู้ร้องขอต้องกรอกแบบฟอร์มเพิ่มเติม ได้แก่ แบบฟอร์มการขอเข้าอาคารเทคโนโลยีสารสนเทศ (วันหยุดราชการ) ให้ผู้ดูแลระบบพิจารณาคำร้องขอ จากนั้นส่งให้เจ้าหน้าที่ส่วนบริหารคอมพิวเตอร์และเครือข่ายพิจารณาอนุมัติ

(๔) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของกรมสรรพสามิตที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบเครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบน้ำและเครื่องดับเพลิง ระบบปรับอากาศและควบคุมความชื้น และต้องมีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านี้อย่างสม่ำเสมอ

เพื่อให้มั่นใจได้ว่า ระบบสนับสนุนทำงานได้เป็นปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบสนับสนุน

(๕) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้อง Data Center ทำงานผิดปกติหรือหยุดการทำงาน

๑.๘.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของกรมสรรพสามิตในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อบนสายสัญญาณและอุปกรณ์

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(๗) สำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๑.๘.๓ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๑) ให้มีการบำรุงรักษาอุปกรณ์ ได้แก่ อุปกรณ์เครือข่าย อุปกรณ์คอมพิวเตอร์ และอุปกรณ์สนับสนุน ตามรอบระยะเวลา และปฏิบัติตามคำแนะนำของผู้ผลิต

(๒) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์ทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๓) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่ตรวจสอบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว โดยกรอกแบบฟอร์มตรวจสอบอุปกรณ์ห้อง Data Center จากนั้นดำเนินการรายงานสรุปผลการเฝ้าระวังเหตุการณ์ให้ผู้บังคับบัญชาและผู้ที่เกี่ยวข้องทราบเป็นประจำทุกเดือน

(๔) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในกรมสรรพสามิต

(๕) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑.๘.๔ การนำสินทรัพย์ของกรมสรรพสามิตออกนอกหน่วยงาน (Removal of Property)

(๑) ต้องขออนุญาตก่อนนำอุปกรณ์หรือสินทรัพย์นั้นออกไปใช้งาน

(๒) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งาน

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ต้องตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของกรมสรรพสามิตออกไปใช้งาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๑.๘.๕ การป้องกันอุปกรณ์ที่นำไปใช้นอกกรมสรรพสามิต (Security of Equipment Off-Premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือสินทรัพย์ของกรมสรรพสามิตออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์ เป็นต้น

(๒) ไม่ทิ้งอุปกรณ์หรือสินทรัพย์ของกรมสรรพสามิตไว้โดยลำพังในที่สาธารณะ

(๓) ให้เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์เสมือนเป็นสินทรัพย์ของตนเอง

๑.๘.๖ การกำจัดอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-Use of Equipment)

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว โดยเมื่อต้องการทำลายสื่อบันทึกข้อมูล หรือถึงรอบการทำลายสื่อบันทึกข้อมูลตามแบบฟอร์มบันทึกรายการสินทรัพย์ผู้ร้องขอต้องกรอกแบบฟอร์มขอทำลายสื่อบันทึกข้อมูล และส่งต่อให้แก่ผู้เชี่ยวชาญด้านพัฒนาความมั่นคงปลอดภัยสารสนเทศหรือเจ้าหน้าที่ส่วนบริหารคอมพิวเตอร์และเครือข่ายที่ได้รับมอบหมาย เพื่อขออนุมัติการทำลายสื่อบันทึกข้อมูล

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๑.๘.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารที่เกี่ยวข้องกับระบบสารสนเทศ

(๑) จัดเก็บเอกสารไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ให้เจ้าของระบบสารสนเทศมีหน้าที่ควบคุมการเข้าถึงและการทำลายเอกสาร

(๓) ให้มีการควบคุมการเข้าถึงเอกสารที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ

(๔) การขอขึ้นทะเบียนเอกสาร ให้ผู้จัดทำเอกสารกรอกแบบฟอร์มคำร้องขอดำเนินการเกี่ยวกับเอกสาร (Document Action Request) เพื่อขึ้นทะเบียนเอกสาร โดยให้ผู้บังคับบัญชาพิจารณาอนุมัติการขึ้นทะเบียนเอกสาร จากนั้นนายทะเบียนเอกสารดำเนินการประกาศให้ผู้ที่เกี่ยวข้องรับทราบ

(๕) การทบทวนเอกสาร ผู้ได้รับมอบหมายให้เป็นผู้ควบคุมทะเบียนเอกสาร แจ้งเจ้าของเอกสารเมื่อถึงรอบการทบทวนเอกสารรับทราบ ผู้จัดทำเอกสารดำเนินการทบทวนเอกสารตามรอบการทบทวน และประกาศผลการทบทวนเอกสาร

๑.๙ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

๑.๙.๑ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(๑) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของกรมสรรพสามิตเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

(๒) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของกรมสรรพสามิต

(๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศ ต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ โดยกรอกแบบฟอร์มขอติดตั้งซอฟต์แวร์ เพื่อให้เจ้าหน้าที่ผู้ดูแลระบบ ตรวจสอบความถูกต้องของลิขสิทธิ์ซอฟต์แวร์ จากนั้นให้เจ้าหน้าที่ส่วนบริหารคอมพิวเตอร์และเครือข่ายพิจารณาอนุมัติการติดตั้งซอฟต์แวร์ โดยหากเจ้าหน้าที่ผู้ดูแลระบบตรวจสอบพบว่าซอฟต์แวร์ที่ขอติดตั้งไม่ถูกลิขสิทธิ์ ให้ระงับการดำเนินการติดตั้งซอฟต์แวร์นั้น

(๔) ไม่ควรติดตั้งซอร์สโค้ด คอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

(๕) กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารี่สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๖) กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้อง ต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย เช่น ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบสารสนเทศ เป็นต้น

(๗) ให้ผู้ที่เกี่ยวข้องดำเนินการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่าย

(๘) ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้น ตามระยะเวลาที่เหมาะสม

(๙) ให้มีการระบุความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ ก่อนที่จะเริ่มต้นทำการพัฒนาหรือปรับปรุงระบบสารสนเทศ

๑.๙.๒ ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศให้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวน ก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่กรมสรรพสามิตต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๑.๙.๓ การควบคุมการพัฒนาซอฟต์แวร์ของผู้รับจ้างจากภายนอก

(๑) ให้มีการควบคุมการพัฒนาซอฟต์แวร์ เช่น ด้านคุณภาพ ด้านความถูกต้องของซอฟต์แวร์ เป็นต้น

(๒) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์

(๓) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๑.๙.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค

ให้ผู้ดูแลระบบ ดำเนินการบริหารจัดการ ดังนี้

(๑) จัดทำบัญชีของระบบสารสนเทศ โดยมีการบันทึกข้อมูลอย่างน้อยดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟแวร์นั้น ๆ

(๒) จัดการกับช่องโหว่ของระบบสารสนเทศอย่างเหมาะสมโดยทันที

(๓) เฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

(๔) กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของกรมสรรพสามิต

(๕) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

(๖) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบหรือเปิดให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้ดูแลระบบเป็นลายลักษณ์อักษร

๑.๙.๕ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) ให้มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ข้อมูลชื่อบัญชีผู้ใช้งาน

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ

(๓) ข้อมูลวันเวลาที่ออกจากระบบ

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๕) ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ

(๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๗) ข้อมูลการเปลี่ยนแปลงคอนฟิกกูเรชั่นของระบบ

(๘) ข้อมูลแสดงการใช้งานแอพพลิเคชัน

(๙) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

(๑๐) ข้อมูลไอพีแอดเดรสที่เข้าถึง

(๑๑) ข้อมูลโพรโตคอลเครือข่ายที่ใช้

(๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

(๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๑.๑๐ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา (Mobile Device)

๑.๑๐.๑ การใช้งานทั่วไป ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) เครื่องคอมพิวเตอร์ที่กรมสรรพสามิตอนุญาตให้ผู้ใช้งาน ใช้งานเป็นสินทรัพย์ของกรมสรรพสามิต ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของกรมสรรพสามิต

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของกรมสรรพสามิต ต้องเป็นโปรแกรมที่กรมสรรพสามิตได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของกรมสรรพสามิต

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับกรมสรรพสามิตเท่านั้น

(๕) ก่อนการใช้งานกับสื่อบันทึกข้อมูลแบบพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสคอมพิวเตอร์โดยโปรแกรมป้องกันไวรัสคอมพิวเตอร์

(๖) ไม่เก็บข้อมูลสำคัญของกรมสรรพสามิตไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่

(๗) ไม่นำอาหาร เครื่องดื่ม หรือสิ่งที่เป็นของเหลว มาวางใกล้บริเวณเครื่องคอมพิวเตอร์

(๘) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

(๙) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากที่สูง เป็นต้น

(๑๐) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๑๑) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

(๑๒) ไม่วางของทับบนเครื่องคอมพิวเตอร์ หรือแป้นพิมพ์

(๑๓) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย เป็นต้น

(๑๔) ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในเครื่องคอมพิวเตอร์รวมถึงแบตเตอรี่

๑.๑๐.๒ การสำรองข้อมูลและการกู้คืน

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

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เนื่องจากหากมีความเสียหายเกิดขึ้นต่อ Hard Disk อาจก่อให้เกิดผลกระทบต่อการดำเนินการของกรมสรรพสามิตได้

๑.๑๑ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ (Information Classification)

๑.๑๑.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๑.๑๑.๒ เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๑.๑๑.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

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

๑.๑๑.๕ ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของกรมสรรพสามิต เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกข้อมูลก่อน เป็นต้น

๑.๑๒ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑.๑๒.๑ ผู้ใช้งาน ต้องดำเนินการดังต่อไปนี้

(๑) ผู้ใช้งานที่ต้องการใช้งานจดหมายอิเล็กทรอนิกส์ของกรมสรรพสามิต ต้องขออนุญาตเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย เพื่อดำเนินการกำหนดสิทธิชื่อผู้ใช้งานรายใหม่และรหัสผ่าน

(๒) เมื่อได้รับรหัสผ่าน จะต้องเปลี่ยนรหัสผ่านโดยทันที หลังจากการเข้าสู่ระบบเป็นครั้งแรก

(๓) ต้องใช้จดหมายอิเล็กทรอนิกส์ของกรมสรรพสามิต เพื่อติดต่องานของราชการเท่านั้น ห้ามใช้เพื่อการประกอบธุรกิจ หรือแสวงหาผลประโยชน์ส่วนตน เผยแพร่ อ้างอิง พาดพิง ดูหมิ่น หรือกระทำใด ๆ ที่ก่อให้เกิดความเสียหายต่อสถาบัน ชาติ ศาสนา และพระมหากษัตริย์ หรือเผยแพร่ข้อมูลข่าวสาร ภาพ เสียง ข้อความ ที่ไม่เหมาะสม แสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบ หรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือองค์กร

(๔) ห้ามใช้ E-Mail Address ของผู้อื่น เพื่ออ่าน หรือรับส่งข้อความ

(๕) หลังจากการใช้งาน ต้องออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งาน

(๖) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

(๗) ควรตรวจสอบและลบจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน เพื่อลดปริมาณการใช้พื้นที่ของระบบ ให้เหลือจำนวนน้อยที่สุด

(๘) ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้ (User Name) และรหัสผ่าน (Password) เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

๑.๑๒.๒ ผู้ดูแลระบบ ต้องดำเนินการดังต่อไปนี้

(๑) กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของกรมสรรพสามิตให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน

(๒) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

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

(๔) มีการควบคุมการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ตามแนวทางการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้อย่างเคร่งครัด

๑.๑๓ การใช้งานระบบอินเทอร์เน็ต (Internet)

๑.๑๓.๑ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่กรมสรรพสามิตจัดสรรไว้เท่านั้น เช่น Proxy Firewall เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-Up Modem เป็นต้น เว้นแต่มีเหตุผลความจำเป็นและได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมายแล้วเท่านั้น

๑.๑๓.๒ จะต้องมีการตั้งค่าเครื่องคอมพิวเตอร์ เพื่อทำการอุดช่องโหว่ ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ต

๑.๑๓.๓ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของกรมสรรพสามิต และต้องไม่ใช้ระบบอินเทอร์เน็ตของกรมสรรพสามิต เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงแห่งชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับกรมสรรพสามิต เป็นต้น

๑.๑๓.๔ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของกรมสรรพสามิต ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๑.๑๓.๕ ห้ามดาวน์โหลดโปรแกรมใช้งาน จากระบบอินเทอร์เน็ตที่เป็นการละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๑.๑๓.๖ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของกรมสรรพสามิต ไม่เสนอความคิดเห็น ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของกรมสรรพสามิต หรือทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๑.๑๓.๗ ผู้ใช้งานต้องทำการปิดเว็บบราวเซอร์เมื่อสิ้นสุดการใช้งาน เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๑.๑๔ การใช้งานอุปกรณ์ป้องกันการบุกรุก (Firewall)

๑.๑๔.๑ ต้องกำหนดเงื่อนไขของการเชื่อมต่อหรือการให้บริการที่ได้รับอนุญาตเท่านั้น โดยกำหนดเงื่อนไขเป็น Deny All Allow Some คือ ห้ามทุกการเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก เว้นแต่จะได้รับการอนุญาต

๑.๑๔.๒ เงื่อนไขการเชื่อมต่อหรือการให้บริการที่กำหนดว่าได้รับอนุญาตให้ผ่านอุปกรณ์ป้องกันการบุกรุกได้ จะต้องบันทึกเป็นเอกสาร และสำเนาให้กับผู้ดูแลระบบรับทราบ โดยเงื่อนไขของการอนุญาตจะต้องได้รับความเห็นชอบจากผู้ดูแลระบบ และรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

๑.๑๔.๓ เส้นทางการสื่อสารคอมพิวเตอร์ที่เข้าออกจากกรมสรรพสามิต จะต้องได้รับการติดตั้งอุปกรณ์ป้องกันการบุกรุกในทุกเส้นทาง

๑.๑๔.๔ เครื่องคอมพิวเตอร์แม่ข่ายที่มีการเชื่อมต่อไปยังภายนอกองค์กร จะต้องจัดให้อยู่ใน DMZ (De-Militarize Zone) เสมอ

๑.๑๔.๕ ต้องไม่อนุญาตให้การสื่อสารจากภายนอกองค์กร ผ่านเข้าไปในองค์กรได้ โดยจะยอมให้เข้ามาในส่วน DMZ ได้เท่านั้น

๑.๑๔.๖ หากมีการเพิ่มเติมหรือเปลี่ยนแปลงเส้นทางการสื่อสารคอมพิวเตอร์ จะต้องได้รับการอนุญาตจากผู้ดูแลระบบก่อน และต้องมีการตรวจสอบผลกระทบกับอุปกรณ์ป้องกันการบุกรุก และเงื่อนไขที่ตั้งให้กับอุปกรณ์ป้องกันการบุกรุก

๑.๑๔.๗ อุปกรณ์ป้องกันการบุกรุกที่นำมาใช้งาน จะต้องทำหน้าที่ป้องกันการบุกรุกเพียงอย่างเดียว โดยไม่ทำหน้าที่อื่น ๆ เช่น AntiVirus Gateway เป็นต้น

๑.๑๔.๘ ผู้ดูแลระบบจะต้องตรวจสอบการทำงานของอุปกรณ์ป้องกันการบุกรุก จากบันทึกการทำงาน (Log File) อย่างสม่ำเสมอ อย่างน้อยทุกสัปดาห์ และรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบเป็นรายเดือน

๑.๑๔.๙ การเปลี่ยนแปลงใด ๆ ที่เกี่ยวกับอุปกรณ์ป้องกันการบุกรุกจะต้องได้รับการบันทึกอย่างน้อยต้องประกอบด้วย การตั้งค่าการเชื่อมต่อ หรือบริการที่ได้รับอนุญาต

๑.๑๔.๑๐ อุปกรณ์ป้องกันการบุกรุกจะต้องได้รับการป้องกันจากการเข้าถึงทางกายภาพ โดยจะต้องติดตั้งในห้องที่มีการรักษาความปลอดภัย มีการล็อก โดยอนุญาตให้ผู้ดูแลระบบเท่านั้นที่สามารถเข้าถึงได้

๑.๑๔.๑๑ ข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่เข้า-ออกอุปกรณ์ป้องกันการบุกรุก จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูล โดยจะต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไม่น้อยกว่า ๙๐ วัน

๑.๑๔.๑๒ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ป้องกันการบุกรุกเป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

๑.๑๔.๑๓ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

๑.๑๔.๑๔ กรมสรรพสามิต มีสิทธิที่จะระงับการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

๑.๑๔.๑๕ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการ ตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

๑.๑๔.๑๖ ผู้ละเมิดนโยบายด้านความปลอดภัยของอุปกรณ์ป้องกันการบุกรุก จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

๑.๑๕ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑.๑๕.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่กรมสรรพสามิตได้กำหนดไว้เท่านั้น

๑.๑๕.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับกรมสรรพสามิตจากการใช้งานเครือข่ายสังคมออนไลน์

๑.๑๕.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับกรมสรรพสามิต ผู้ใช้งานต้องแจ้งต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑.๑๖ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

๑.๑๖.๑ ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บ กำหนดชั้นความลับในการเข้าถึง

๑.๑๖.๒ ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้

๑.๑๖.๓ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า – ออกระบบ บันทึกการ

พยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

๑.๑๖.๔ ต้องมีวิธีป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ได้แก่ ผู้ตรวจสอบระบบสารสนเทศของกรมสรรพสามิต (IT Auditor) หรือบุคคลที่กรมสรรพสามิตมอบหมาย

๑.๑๗ นโยบายการเข้ารหัสข้อมูลและการบริหารจัดการกุญแจเข้ารหัสข้อมูล (Cryptographic Control)

ผู้ดูแลระบบ ต้องกำหนดให้มีแนวทางการบริหารจัดการกุญแจ (Key) ที่ใช้เข้ารหัสข้อมูล เพื่อรองรับการใช้งานเทคนิคที่เกี่ยวข้องกับการเข้ารหัสลับของกรมสรรพสามิต โดยให้มีการควบคุม กำกับ ติดตาม ให้ครอบคลุมตลอดทั้งวงจรในการนำกุญแจรหัสลับ ไปใช้งาน ได้แก่ การสร้างกุญแจรหัสลับ การจัดเก็บและดูแลรักษากุญแจรหัสลับ การนำกุญแจรหัสลับไปใช้ การกำหนดอายุของกุญแจรหัสลับ ตลอดจนการทำลายกุญแจรหัสลับเมื่อไม่ได้ใช้งาน

๑.๑๘ นโยบายการดำเนินงานร่วมกับหน่วยงานภายนอก (Supplier relationship Management)

๑.๑๘.๑ ต้องควบคุมให้มีการจัดทำข้อตกลงด้านการรักษาความลับของข้อมูล (Non-disclosure agreement - NDA) กับผู้ให้บริการภายนอก รวมทั้งการกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศในขอบเขตงานและเงื่อนไขในการให้บริการ (Service level agreement - SLA)

๑.๑๘.๒ ต้องกำกับให้มีการดูแลให้บุคคลหรือหน่วยงานภายนอกที่ให้บริการแก่กรมสรรพสามิตตามที่ว่าจ้าง ปฏิบัติตามสัญญาหรือข้อตกลงให้บริการที่ระบุไว้ ซึ่งต้องครอบคลุมถึงงานด้านความมั่นคงปลอดภัยสารสนเทศ

๑.๑๘.๓ ต้องควบคุมให้มีการกำหนดข้อตกลงและความรับผิดชอบที่เกี่ยวข้องกับความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศลงในสัญญากับผู้ให้บริการภายนอกที่ให้บริการด้านสารสนเทศ และบริการด้านการสื่อสาร โดยให้ครอบคลุมรวมถึงผู้รับจ้างช่วง

๑.๑๙ การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)

๑.๑๙.๑ การใช้งานทั่วไป ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) ไม่เปิดอ่านจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือเปิดเอกสารแนบ หรือลิงก์ใด ๆ ที่ได้รับทางจดหมายอิเล็กทรอนิกส์ (E-Mail) จากบุคคลที่ไม่รู้จักหรือไม่เคยติดต่อ หากเป็นจดหมายอิเล็กทรอนิกส์ (E-Mail) จากบุคคลที่รู้จักหรือเคยติดต่อแล้วนั้น ผู้ใช้งานต้องตรวจสอบความถูกต้องของจดหมายอิเล็กทรอนิกส์ (E-Mail) นั้น ให้ถูกต้องทุกครั้งก่อนตอบกลับหรือให้ข้อมูลใด ๆ กรณีมีความจำเป็นต้องส่งข้อมูลสำคัญ ควรมีการเข้ารหัสข้อมูลอย่างเหมาะสม และยืนยันการรับส่งข้อมูลกับผู้รับปลายทางทุกครั้ง

(๒) ไม่เปิดเผยข้อมูลส่วนบุคคล และข้อมูลสำคัญของกรมสรรพสามิต ผ่านช่องทางต่าง ๆ เช่น เว็บไซต์ เครือข่ายสังคมออนไลน์ (Social Network) Internet Messaging เป็นต้น

(๓) ไม่เข้าใช้งานเข้าเว็บไซต์ที่ไม่เหมาะสม และไม่ดาวน์โหลดไฟล์หรือซอฟต์แวร์จากเว็บไซต์ที่ไม่น่าเชื่อถือ เพื่อหลีกเลี่ยงผลกระทบที่เกิดจากซอฟต์แวร์ไม่พึงประสงค์ (Malware)

(๔) สำรองข้อมูลสำคัญอย่างสม่ำเสมอ และจัดเก็บข้อมูลที่สำรองไว้ในพื้นที่จัดเก็บที่มีความปลอดภัย หรือเข้ารหัสอย่างเหมาะสม

(๕) กรณีที่พบภัยคุกคามหรือช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ ต้องรายงานให้ผู้ดูแลระบบได้รับทราบ เพื่อดำเนินการแก้ไขหรือปรับปรุงอย่างทันท่วงที

๑.๑๙.๒ เพื่อให้กรมสรรพสามิตสามารถตรวจจับ ป้องกันและรับมือเหตุการณ์ผิดปกติได้อย่างทันท่วงที โดยมีกระบวนการติดตามดูแลความมั่นคงปลอดภัยของระบบ รวมถึงเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง ผู้ดูแลระบบต้องดำเนินการ ดังต่อไปนี้

(๑) ต้องกำหนดกระบวนการในการติดตาม ดูแลระบบ และเฝ้าระวังภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้มีการติดตามดูแลความปลอดภัยของระบบอย่างต่อเนื่อง

(๒) ต้องมีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความปลอดภัยของระบบที่สำคัญ โดยต้องครอบคลุมระบบงานและระบบเครือข่ายสื่อสาร เพื่อให้ผู้ที่เกี่ยวข้องรับทราบถึงความผิดปกติ หรือภัยคุกคามอย่างทันท่วงที และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม

(๓) ต้องกำหนดผู้รับผิดชอบในการประสานงานเพื่อแลกเปลี่ยนข้อมูลภัยคุกคามระหว่างกรมสรรพสามิตและหน่วยงานที่เกี่ยวข้อง รวมทั้งมีกระบวนการและช่องทางในการรายงาน แลกเปลี่ยน ติดตาม เพื่อป้องกันรับมือและแก้ไขภัยคุกคาม

(๔) ในกรณีที่พบภัยคุกคามที่ส่งผลกระทบอย่างมีนัยสำคัญ ต้องรายงานภัยคุกคามดังกล่าวให้คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศได้รับทราบ รวมถึงดำเนินการวิเคราะห์เพื่อให้ทราบสาเหตุ หรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่และป้องกันความเสี่ยงที่อาจเกิดขึ้นอีก

๒. แนวปฏิบัติระบบสำรองของสารสนเทศ และแผนเตรียมความพร้อมกรณีฉุกเฉิน

เพื่อให้ระบบสารสนเทศของกรมสรรพสามิตสามารถให้บริการได้อย่างต่อเนื่อง จึงกำหนดแนวปฏิบัติระบบสำรองของระบบสารสนเทศ และแผนเตรียมความพร้อมกรณีฉุกเฉิน โดยมอบหมายให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ ดังนี้

๒.๑ ผู้ดูแลระบบต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๒.๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของกรมสรรพสามิต พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๒.๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลการคอนฟิกกูเรชัน ข้อมูลในฐานข้อมูล เป็นต้น

- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับกรมสรรพสามิตควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับกรมสรรพสามิต เช่น ไฟไหม้ เป็นต้น

- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

- ทดสอบบันทึกข้อมูลที่สำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

- กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๒.๒ ให้กรมสรรพสามิตจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

๒.๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๒.๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๒.๓ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๒.๔ ผู้ดูแลระบบต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๕ ผู้ดูแลระบบมีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ของกรมสรรพสามิต ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ อย่างน้อยปีละ ๑ ครั้ง

๒.๖ ผู้ดูแลระบบต้องกำหนดชนิดของข้อมูลและระยะเวลาที่ต้องการจะสำรองข้อมูล ว่าข้อมูลที่ต้องการสำรองเป็นข้อมูลชนิดใด และต้องใช้พื้นที่สำหรับการสำรองข้อมูลเท่าใด

๒.๗ ผู้ดูแลระบบจัดทำการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายที่มีความสำคัญโดยมีการสำรองแบบเต็มรูปแบบ (Full Backup) อย่างน้อยเดือนละ ๑ ครั้ง โดยกำหนดให้เป็นวันศุกร์แรกของเดือนหรือวันอื่นตามความเหมาะสม

๒.๘ ผู้ดูแลระบบต้องจัดทำการสำรองข้อมูลแบบบางส่วน (Incremental Backup) อย่างน้อยสัปดาห์ละ ๑ ครั้ง

๒.๙ ผู้ดูแลระบบต้องจัดทำการทดสอบการกู้กลับคืนของข้อมูล (Restore) ทุก ๖ เดือน

๒.๑๐ ผู้ดูแลระบบต้องจัดให้มีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

๒.๑๑ ข้อมูลที่สำรองและถูกจัดลำดับความสำคัญมากที่สุด ต้องมีการสำรองข้อมูลมากกว่า ๑ ชุด และต้องทำการสำรองข้อมูลไปยังสถานที่อื่นเพื่อความปลอดภัย

๓. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ และเพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ จึงกำหนดแนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมอบหมายให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และผู้ตรวจสอบภายใน (Internal Auditor) แต่งตั้งโดยกรมสรรพสามิต และผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ ดังนี้

๓.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) โดยผู้ตรวจสอบภายใน (Internal Auditor) แต่งตั้งโดยกรมสรรพสามิต อย่างน้อยปีละ ๑ ครั้ง เพื่อให้กรมสรรพสามิตได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๓.๒ แนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง มีดังนี้

๓.๒.๑ ต้องมีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๒ ต้องมีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๓ ต้องมีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๓.๒.๔ ต้องมีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ต้องแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต