ประกาศสำนักบริหารการทะเบียน
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักบริหารการทะเบียน
พ.ศ. ๒๕๖๕

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ผู้อำนวยการสำนักบริหารการทะเบียน จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักบริหารการทะเบียน เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน พ.ศ. ๒๕๖๕”

ข้อ ๒ ในประกาศนี้

(๑) **หน่วยงาน** หมายความว่า สำนักบริหารการทะเบียน

(๒) **ผู้บริหาร** หมายความว่า ผู้อำนวยการสำนักบริหารการทะเบียนหรือผู้ที่ผู้อำนวยการสำนักบริหารการทะเบียนมอบหมายให้ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศของหน่วยงาน

(๓) **ผู้บริหารระดับสูงสุด** หมายความว่า ผู้อำนวยการสำนักบริหารการทะเบียน

(๔) **คณะกรรมการ** หมายความว่า คณะกรรมการนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๕) **คณะทำงาน** หมายความว่า คณะทำงานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๖) **นโยบาย** (Policy) หมายความว่า นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๗) **ผู้ใช้งาน** (User) หมายความว่า ข้าราชการ พนักงานราชการ เจ้าหน้าที่ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารของหน่วยงาน รวมถึงบุคคลภายนอกที่สังกัดส่วนราชการหรือหน่วยงานของรัฐ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

(๘) **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

(๙) **สินทรัพย์** (Asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับหน่วยงาน

(๑๐) **สินทรัพย์สารสนเทศ** หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล อุปกรณ์อื่นที่เกี่ยวข้องกับสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

/(๑๐) **การเข้าถึง**...

(๑๑) **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๑๒) **ความมั่นคงปลอดภัยด้านสารสนเทศ** (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

(๑๓) **เหตุการณ์ด้านความมั่นคงปลอดภัย** (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

(๑๔) **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๓ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๔

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๕ ถึงข้อ ๑๑

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้มี ๒ ส่วน ดังนี้

(๑) ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑.๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานมีส่วนร่วมในการทำนโยบาย

(๑.๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของหน่วยงาน

(๑.๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๑.๔) ต้องทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

(๒) ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๒.๑) การเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ มีนโยบายให้บริการระบบสารสนเทศแก่ผู้ดูแลระบบ ผู้ใช้งาน โดยสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวก รวดเร็ว และให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย ภายใต้บทบัญญัติของกฎหมาย

(๒.๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีระบบแยกประเภทและจัดเก็บเป็นหมวดหมู่ มีระบบสำรองของสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์และสภาพพร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง

/(๒.๓) การตรวจสอบ...

(๒.๓) การตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศอย่างสม่ำเสมอ มีนโยบายให้มีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

(๒.๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือการใช้งาน และการจัดการฝึกอบรมหรือเผยแพร่การใช้งานระบบสารสนเทศทางเว็บไซต์ภายใน (Intranet) และเว็บไซต์ภายนอก (Internet) ของหน่วยงานแก่ผู้ดูแลระบบ และผู้ใช้งาน

ข้อ ๕ ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

(๑) ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ

(๒) กำหนดหลักเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่เข้าถึงได้ และช่องทางการเข้าถึง

(๔) มีวิธีการบริหารจัดการการเข้าถึงข้อมูลสารสนเทศและระบบสารสนเทศของผู้ใช้งานแต่ละประเภทที่เหมาะสมและตรวจสอบได้ เพื่อป้องกันการเข้าถึงผู้ไม่ได้รับอนุญาต โดยครอบคลุมการลงทะเบียน การจัดการสิทธิผู้ใช้งาน รหัสผ่าน การทบทวนสิทธิการใช้งาน เพื่อให้มั่นใจว่าสอดคล้องกับภาระหน้าที่และความจำเป็นในการใช้งาน

(๕) ต้องควบคุมการเข้าถึงเครือข่ายและการใช้บริการผ่านเครือข่าย รวมทั้งการเชื่อมต่อเครือข่ายทั้งจากภายในหน่วยงานและจากภายนอกหน่วยงาน เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศหรือระบบสารสนเทศโดยไม่ได้รับอนุญาต

(๖) ต้องควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการใช้งานอุปกรณ์เพื่อการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

(๗) ต้องควบคุมการเข้าถึงโปรแกรมและระบบสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

ข้อ ๖ ต้องบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน ต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อต้องอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อยกเลิกการอนุญาตดังกล่าว

(๓) การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัยโดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

/ข้อ ๗ ต้องกำหนด...

ข้อ ๗ ต้องกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหา ดังนี้

(๑) การใช้งานรหัสผ่าน กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน ต้องกำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อไม่ใช้งาน

ข้อ ๘ การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองของสารสนเทศ ให้อยู่ในสภาพพร้อมใช้งาน

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการทำงานตามภารกิจ

(๓) ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศและระบบสำรองของสารสนเทศ

(๔) ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองของสารสนเทศและแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) ต้องปฏิบัติและทบทวนแนวทางการจัดทำระบบสำรองของสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ การตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ โดยมีเนื้อหา ดังนี้

(๑) ต้องกำหนดวิธีการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ

(๒) ต้องกำหนดให้ตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ ปีละ ๑ ครั้ง

(๓) ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบในการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ

(๔) ต้องมีการรายงานผลการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๐ ต้องประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติ ด้วยวิธีการใดวิธีการหนึ่ง ดังนี้

(๑) หนังสือเวียนภายในหน่วยงาน

(๒) เว็บไซต์ของหน่วยงาน

ข้อ ๑๑ ส่วนงานภายในหน่วยงานที่ต้องบริหารจัดการระบบเทคโนโลยีสารสนเทศสามารถกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานได้เอง ทั้งนี้ ต้องให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน พ.ศ. ๒๕๖๕

/**ข้อ ๑๒** กำหนดให้...

ข้อ ๑๒ กำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงาน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศที่มีความสำคัญเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงาน หรือผู้ใดผู้หนึ่ง อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑๓ กำหนดบทบาทหน้าที่ผู้รับผิดชอบตามนโยบายและแนวปฏิบัติ ดังนี้

(๑) คณะกรรมการ มีหน้าที่กำกับดูแลการใช้งานระบบสารสนเทศให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๒) คณะทำงาน มีหน้าที่จัดทำและทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๓) ผู้ดูแลระบบ มีหน้าที่ดูแล ติดตาม และตรวจสอบ การใช้งานระบบสารสนเทศให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

(๔) ผู้ใช้งาน เป็นผู้เข้าถึงและใช้งานระบบสารสนเทศของสำนักบริหารการทะเบียน ตามสิทธิที่ได้รับอนุญาต โดยให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

ข้อ ๑๔ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๑ มิถุนายน พ.ศ. ๒๕๖๕

(นายสุชาติ ธานีรัตน์)
ผู้อำนวยการสำนักบริหารการทะเบียน

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักบริหารการทะเบียน
พ.ศ. ๒๕๖๕

เอกสารหมายเลข ๑	**คำนิยาม**
เอกสารหมายเลข ๒	**นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักบริหารการทะเบียน**
เอกสารหมายเลข ๓	**แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) สำนักบริหารการทะเบียน**

คำนิยาม

๑. **หน่วยงาน** หมายความว่า สำนักบริหารการทะเบียน

๒. **หน่วยงานภายใน** หมายความว่า สำนักงานผู้เชี่ยวชาญ ส่วน กลุ่มงานบริหารทั่วไป ศูนย์บริหารการทะเบียนภาค ศูนย์บริหารการทะเบียนภาค สาขาจังหวัด หรือหน่วยงานที่เรียกชื่อเป็นอย่างอื่นในสังกัดสำนักบริหารการทะเบียน

๓. **หน่วยงานภายนอก** หมายความว่า หน่วยงานราชการ รัฐวิสาหกิจ หรือองค์กรที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๔. **ผู้ใช้งาน (User)** หมายความว่า ข้าราชการ พนักงานราชการ เจ้าหน้าที่ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารของหน่วยงาน รวมถึงบุคคลภายนอกที่สังกัดส่วนราชการหรือหน่วยงานของรัฐ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน

๕. **ชื่อผู้ใช้ (Username)** หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่ได้กำหนดสิทธิการใช้งานไว้

๖. **รหัสผ่าน (Password)** หมายความว่า กลุ่มตัวอักษรหรือตัวเลขหรืออักขระ รวมถึงรหัสลับ (PINCODE) ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลสารสนเทศ ระบบสารสนเทศ และระบบเครือข่าย

๗. **บัญชีผู้ใช้ (Account)** หมายความว่า รายชื่อผู้ใช้และรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๘. **ระบบคอมพิวเตอร์** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๙. **อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่** หมายความว่า อุปกรณ์คอมพิวเตอร์ทุกชนิดและอุปกรณ์สื่อสารที่สามารถนำไปติดตั้งนอกสถานที่ได้ อุปกรณ์สื่อสารแบบพกพา เช่น สมาร์ทโฟน แท็บเล็ต รวมถึงอุปกรณ์อิเล็กทรอนิกส์ที่ทำหน้าที่ได้เหมือนคอมพิวเตอร์ และอุปกรณ์ที่เชื่อมต่อหรือทำงานเป็นส่วนหนึ่งของระบบคอมพิวเตอร์โดยอาจใช้ทำหน้าที่เป็นอุปกรณ์สื่อสาร หรือใช้บันทึกข้อมูล เช่น เครื่องพิมพ์ สแกนเนอร์ หน่วยความจำภายนอก โทรศัพท์ กล้องดิจิทัล โทรทัศน์อัจฉริยะ และอุปกรณ์เครือข่ายต่าง ๆ เป็นต้น

๑๐. **ข้อมูล (Data)** หมายความว่า ข้อเท็จจริงที่เป็นตัวเลข ข้อความ ภาพ เสียง วิดีโอ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ รวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๑. **สารสนเทศ (Information)** หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๑๒. **ระบบสารสนเทศ (Information System)** หมายความว่า ระบบที่ประกอบด้วยส่วนต่างๆ ได้แก่ ระบบคอมพิวเตอร์ ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย ฐานข้อมูล ผู้พัฒนาระบบ ผู้ใช้งานระบบ พนักงานที่เกี่ยวข้อง และผู้เชี่ยวชาญในสาขา ทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูล เพื่อสร้างสารสนเทศและส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้งานเพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม

๑๓. **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายความว่า เครื่องคอมพิวเตอร์ระบบงาน เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่ายและ/หรือ ระบบหรืออุปกรณ์สนับสนุนการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

๑๔. **การเข้าถึง (Access)** หมายความว่า การอนุญาต หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงระบบสารสนเทศและระบบเครือข่าย

๑๕. **การควบคุมการใช้งาน (Access Control)** หมายความว่า การกำหนดสิทธิในการเข้าถึงหรือใช้งานระบบสารสนเทศและระบบเครือข่าย

๑๖. **การพิสูจน์ยืนยันตัวตน (Authentication)** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานระบบ โดยทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้งาน รหัสผ่าน หรือระบบการพิสูจน์ยืนยันตัวตนอื่นใดตามที่หน่วยงานกำหนด

๑๗. **ลงบันทึกการเข้า (Login)** หมายความว่า กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้ระบบคอมพิวเตอร์หรือระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้งาน และรหัสผ่านให้ถูกต้อง

๑๘. **ลงบันทึกการออก (Logout)** หมายความว่า กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์หรือระบบเครือข่าย

๑๙. **การเข้ารหัส (Encryption)** หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๒๐. **ผู้ดูแลระบบ (System Administrator)** หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บริหารให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๒๑. **สื่อบันทึกข้อมูล** หมายความว่า สื่อทั้งที่เป็นอิเล็กทรอนิกส์และไม่เป็นอิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD, DVD, Flash Drive, Handy Drive, Thumb Drive, Hard Drive, Portable Hard Drive, โทรศัพท์มือถือ กล้องถ่ายรูปดิจิตอล กล้องวิดีโอ หรือ เครื่องบันทึกเสียง เป็นต้น

๒๒. **จดหมายอิเล็กทรอนิกส์ (Electronic Mail: E-Mail)** หมายความว่า ระบบรับส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเทคโนโลยีสารสนเทศ ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพนิ่ง ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน

๒๓. **อุปกรณ์จัดเส้นทาง (Router)** หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

๒๔. **อุปกรณ์กระจายสัญญาณ (Access Point)** หมายความว่า อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

๒๕. **หมายเลขไอพีแอดเดรส (IP Address)** หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่เชื่อมต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วนหรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

๒๖. **อัพเดท (Update)** หมายความว่า ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่าง ๆ ของระบบสารสนเทศให้ทันสมัยอยู่เสมอ

๒๗. **ช่องโหว่ (Vulnerability)** หมายความว่า ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๒๘. **VPN (Virtual Private Network)** หมายความว่า เครือข่ายส่วนตัวเสมือน โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๒๙. **SSID (Service Set Identifier)** หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

๓๐. **WEP (Wire Equivalent Privacy)** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

๓๑. **WPA (Wi-Fi Protected Access)** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

๓๒. **MAC Address (Media Access Control Address)** หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขที่จะมากับอีเทอร์เน็ตการ์ดโดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

๓๓. **ไฟร์วอลล์ (Firewall)** หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๓๔. **เครือข่าย (Network)** หมายความว่า โครงข่ายคอมพิวเตอร์ที่เชื่อมโยงคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่าง ๆ เข้าด้วยกัน ซึ่งทำให้การสื่อสารข้อมูลระหว่างคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งที่อยู่ภายในและภายนอกองค์กรสามารถติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้ โครงข่ายนี้โดยพื้นฐานประกอบด้วยโครงข่ายสำหรับการติดต่อสื่อสารภายในองค์กร และโครงข่ายบนอินเทอร์เน็ตซึ่งทำให้คอมพิวเตอร์ภายในองค์กรหนึ่งสามารถติดต่อสื่อสารกับคอมพิวเตอร์ขององค์กรหนึ่งได้

๓๕. **อินเทอร์เน็ต (Internet)** หมายความว่า เครือข่ายของคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายทั่วโลกเข้าด้วยกัน โดยอาศัยเครือข่ายโทรคมนาคมเป็นตัวเชื่อมโยง

๓๖. **อินทราเน็ต (Intranet)** หมายความว่า ระบบเครือข่ายภายในองค์กร เป็นบริการและการเชื่อมต่อคอมพิวเตอร์เหมือนกันอินเทอร์เน็ต แต่จะเปิดให้ใช้เฉพาะสมาชิกในองค์กรเท่านั้น

๓๗. **แผนผังระบบเครือข่าย (Network Diagram)** หมายความว่า แผนผังหรือแผนภาพที่แสดงรูปแบบการจัดวางอุปกรณ์เครือข่ายในระบบเครือข่ายที่แสดงการเชื่อมโยง เพื่อให้เห็นเส้นทางการไหลเวียนของข้อมูลในเครือข่าย

๓๘. **ข้อมูลจราจรทางคอมพิวเตอร์ (Log)** หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

๓๙. **เครือข่ายสังคมออนไลน์ (Social Network)** หมายความว่า เว็บไซต์หรือแอพพลิเคชันที่ผู้ใช้งานสามารถนำเสนอและเผยแพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะโดยใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประเภทต่าง ๆ

๔๐. **ระบบสำรอง (Disaster Recovery Site: DR Site)** หมายความว่า ระบบคอมพิวเตอร์สำรองซึ่งประกอบด้วยฮาร์ดแวร์ซอฟต์แวร์ อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายที่จำเป็น ที่สามารถทำงานได้ทันทีที่ระบบหลักมีปัญหา

๔๑. **การสำรองข้อมูล (Backup)** หมายความว่า การคัดลอกแฟ้มข้อมูลเพื่อทำสำเนา เพื่อหลีกเลี่ยงความเสียหายที่จะเกิดขึ้นหากข้อมูลเกิดการเสียหายหรือสูญหาย โดยสามารถนำข้อมูลที่สำรองไว้มาใช้งานได้ทันที

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ของสำนักบริหารการทะเบียน

พ.ศ. ๒๕๖๕

สารบัญ

หน้า

ความเป็นมา

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ ต้องได้รับความเห็นชอบจากคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์หรือหน่วยงานที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มอบหมายก่อน จึงมีผลใช้บังคับได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๕๓ กำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ และกำหนดให้หน่วยงานภาครัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

สำนักบริหารการทะเบียน จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์ การปฏิบัติงานและบริหารราชการได้อย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยเชื่อถือได้ และสามารถดำเนินงานได้อย่างต่อเนื่อง

๒. วัตถุประสงค์

เพื่อให้บุคลากรทุกระดับที่เกี่ยวข้องได้นำไปปฏิบัติอย่างเคร่งครัด สำนักบริหารการทะเบียน ได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีวัตถุประสงค์ ดังนี้

๒.๑ เพื่อให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน ซึ่งเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๒ เพื่อกำหนดแนวทางและวิธีการปฏิบัติให้บุคลากรและบุคคลที่ปฏิบัติงานให้กับสำนักบริหารการทะเบียน ในการยืนยันตัวบุคคล การเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ

๒.๓ เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ รักษาความถูกต้องสมบูรณ์ความพร้อมใช้อยู่เสมอของระบบสารสนเทศ และมีแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๒.๔ เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศอย่างสม่ำเสมอ

๒.๕ เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ สร้างความเข้าใจและให้การอบรมทางด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศให้แก่บุคลากรและบุคคลที่เกี่ยวข้อง

๓. เป้าหมาย

เป้าหมายในการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน มีรายละเอียดดังนี้

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของสำนักบริหารการทะเบียน

๓.๒ เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๓.๓ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

๓.๔ เผยแพร่ความรู้ความเข้าใจ เพื่อสร้างความตระหนักให้บุคลากรและผู้เกี่ยวข้องทุกระดับในส่วนของสำนักบริหารการทะเบียน หน่วยงานภายในและหน่วยงานภายนอกที่เกี่ยวข้อง

๔. องค์ประกอบนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักบริหารการทะเบียน จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยมีรายละเอียดดังต่อไปนี้

ส่วนที่ ๑ นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Information Access Control)

๒. การบริหารจัดการควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๕. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๘. การควบคุมการเข้าถึงเครือข่ายไร้สาย (Wireless LAN Access Control)

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

๑๐. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

๑๑. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๒. การใช้งานระบบอินเทอร์เน็ต (Internet)

๑๓. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๔. การใช้ห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

๑๕. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator)

๑๖. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log Management)

ส่วนที่ ๒ นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

๑. การคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๒. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

๑. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๒. การดำเนินการตรวจสอบและประเมินความเสี่ยง

๓. การบริหารความต่อเนื่องของระบบสารสนเทศ

๔. การแจ้งเหตุด้านความมั่นคงปลอดภัย

ส่วนที่ ๔ นโยบายสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

การฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน

ส่วนที่ ๑

นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของหน่วยงาน

๒. เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องทุกฝ่าย ได้รับรู้ เข้าใจขั้นตอนและปฏิบัติตามแนวทางบริหารจัดการบัญชีผู้ใช้สารสนเทศของหน่วยงานและถือปฏิบัติโดยเคร่งครัด รวมทั้งสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

ผู้รับผิดชอบ

๑. ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ผู้ใช้งาน

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ (Information Access Control)

๑.๑ จัดทำบัญชีสินทรัพย์หรือทะเบียนสินทรัพย์ การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ดังนี้

- อ่านได้อย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไขข้อมูล
- อนุมัติการใช้ข้อมูล
- ไม่มีสิทธิ

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

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักหรือผู้อำนวยการส่วนที่ได้รับมอบหมาย

๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูล แบ่งออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรองการปฏิบัติราชการ ข้อมูลบุคลากร ข้อมูลงบประมาณ การเงินและบัญชี ข้อมูลสถิติการทะเบียน เป็นต้น
- ข้อมูลสารสนเทศด้านการบริการ เช่น ข้อกฎหมายน่ารู้ กฎหมายและกฎระเบียบข้อมูลกฎหมายทางการทะเบียน เป็นต้น

(๒) จัดแบ่งระดับความสำคัญของข้อมูล แบ่งออกเป็น

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล แบ่งออกเป็น

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

(๔) จัดแบ่งระดับชั้นการเข้าถึง แบ่งออกเป็น

- เข้าถึงได้เฉพาะผู้มีสิทธิสูงสุดในการบริหารจัดการระบบสารสนเทศ
- เข้าถึงได้เฉพาะผู้ใช้งานที่ได้รับอนุมัติสิทธิจากเจ้าของระบบงานแล้วเท่านั้น
- เข้าถึงได้เฉพาะกลุ่มที่เกี่ยวข้อง
- เข้าถึงได้ทุกกลุ่มผู้ใช้งานที่กำหนดไว้แล้ว

(๕) การกำหนดเวลาที่เข้าถึงได้ แบ่งออกเป็น

- ในเวลาราชการ ได้แก่ จันทร์ – ศุกร์ เวลา ๐๘.๓๐ – ๑๖.๓๐ น.
- นอกเวลาราชการที่ได้รับอนุญาต ได้แก่ จันทร์ – ศุกร์ เวลา ๑๖.๓๐ – ๒๐.๓๐ น.
- วันหยุดราชการและวันหยุดนักขัตฤกษ์ที่ได้รับอนุญาต ได้แก่ เวลา ๐๘.๓๐ – ๑๖.๓๐ น.
- เวลาอื่นตามที่ระบุไว้ให้เข้าถึงได้

(๖) การกำหนดช่องทางที่สามารถเข้าถึงได้ แบ่งออกเป็น

- อินทราเน็ต (Intranet)
- อินเทอร์เน็ต (Internet)
- จดหมายอิเล็กทรอนิกส์ (E-Mail)

๒. การบริหารจัดการควบคุมการเข้าถึงสารสนเทศ (Business Requirement for Access Control)

เพื่อควบคุมการเข้าถึงสารสนเทศตามภารกิจให้ปฏิบัติ ดังนี้

๒.๑ มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

๒.๒ มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒.๓ ผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศได้ ต้องมีการบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และเฝ้าระวังการละเมิดความปลอดภัยที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ให้ดำเนินการดังนี้

๓.๑ มีการประชาสัมพันธ์เผยแพร่ความรู้เกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness)

๓.๒ มีการฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งานเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Training) เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึง การณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๓.๓ มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User Registration) ดังนี้

(๑) ผู้ดูแลระบบจัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม โดยระบุข้อมูลพื้นฐาน เช่น ชื่อ-นามสกุล ตำแหน่ง หน่วยงาน

(๒) ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มขอใช้ระบบงานสารสนเทศแล้ว ต้องให้ผู้บังคับบัญชาระดับผู้อำนวยการส่วนหรือเทียบเท่าให้ความเห็นชอบ

(๓) ผู้ดูแลระบบต้องตรวจสอบและกำหนดสิทธิที่เหมาะสมในการเข้าถึงตามหน้าที่ความรับผิดชอบ

(๔) ผู้ดูแลระบบจัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งผู้ขอใช้งานต้องลงนามรับทราบด้วย

(๕) ผู้ดูแลระบบกำหนดชื่อผู้ใช้ (Username) จากชื่อภาษาอังกฤษและตามด้วยอักษรตัวแรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๖) ผู้ดูแลระบบทำการบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้งานระบบสารสนเทศและให้เก็บย้อนหลังอย่างน้อย ๑ ปี

(๗) ผู้ดูแลระบบกำหนดให้มีการยกเลิกหรือเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศเมื่อได้รับแจ้งจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร

๓.๔ มีการกำหนดการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดสิทธิการใช้งานระบบสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(๒) ผู้ดูแลระบบต้องมอบหมายสิทธิให้มีความสอดคล้องกับนโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

(๓) ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศให้เหมาะสมตามหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน

(๔) ผู้ดูแลระบบทำการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งานเป็นลายลักษณ์อักษรและให้เก็บย้อนหลังอย่างน้อย ๑ ปี

(๕) ผู้ดูแลระบบที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศได้

(๖) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ดูแลระบบ หรือผู้ใช้งานอื่นใดที่มีสิทธิในระดับสูง ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกว่าวหรือพ้นจากตำแหน่ง และกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงในระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

๓.๕ มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราวที่ยากต่อการเดา และต้องมีความแตกต่างกัน

(๓) ผู้ดูแลระบบต้องกำหนดวันหมดอายุอย่างน้อยทุก ๒ เดือน สำหรับรหัสผ่านของผู้ใช้งานทุกคน

(๔) ผู้ดูแลระบบต้องส่งมอบบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(๕) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๖) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานลงนาม เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน เช่น ลงนามในเอกสารเพื่อแสดงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ในการเข้าถึงระบบสารสนเทศ

(๗) ผู้ดูแลระบบต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

๓.๖ ข้อกำหนดการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศหรือการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๔.๑ มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนหัสผ่านที่มีความมั่นคงปลอดภัย ดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ควรตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๓) ควรกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๔) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๕) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๙) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(๑๐) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๑) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๒) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน

(๑๔) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๕) ผู้ดูแลระบบต้องเปลี่ยนรหัส ถี่กว่าผู้ใช้งานทั่วไป

๔.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(๑) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๓) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

(๔) ผู้ใช้งานต้องตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๑๕ นาที โดยต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๕) ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๖) ผู้ใช้งานต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

๔.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ดังนี้

(๑) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

- โปรแกรมที่ได้ถูกติดตั้งลงเครื่องคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย โดยห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้บุคคลอื่นใช้งานโดยผิดกฎหมาย
- ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของหน่วยงาน
- ปิดเครื่องคอมพิวเตอร์ (Log Off) ทุกครั้งหลังเลิกงานหรือไม่ใช้งาน
- ออกจากระบบ (Log Out) ออกจากระบบสารสนเทศหรือระบบคอมพิวเตอร์ทันที เมื่อใช้งานเสร็จหรือจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- การส่งเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงานไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน คู่สัญญาเช่าหรือผู้รับจ้างในการบำรุงรักษาหรือซ่อมแซมเครื่องคอมพิวเตอร์และอุปกรณ์ โดยมีข้อตกลงเป็นหนังสือกับหน่วยงานเท่านั้น
- ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่
- ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive
- การใช้เครื่องคอมพิวเตอร์เป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานอีกครั้ง
- ไม่วางของทับบนหน้าจอหรือแป้นพิมพ์
- ให้ติดตั้งหรือจัดเก็บอุปกรณ์คอมพิวเตอร์บนชั้นวางคอมพิวเตอร์ ตู้ติดตั้งอุปกรณ์เครือข่าย กล่องใส่แผ่น CD/DVD หรือสิ่งอื่นใดที่เป็นอุปกรณ์เฉพาะสำหรับติดตั้งหรือเก็บรักษาที่มั่นคงแข็งแรง

- ตรวจสอบ สายไฟ สายเมาส์ สายแป้นพิมพ์ หรือสายสัญญาณของอุปกรณ์คอมพิวเตอร์อื่นใดให้เรียบร้อย เพื่อความเป็นระเบียบและป้องกันอุบัติเหตุที่อาจทำให้อุปกรณ์คอมพิวเตอร์ได้รับความเสียหาย

- ทำความสะอาดอุปกรณ์คอมพิวเตอร์อย่างสม่ำเสมอ เพื่อป้องกันฝุ่นละอองที่จะทำให้เครื่องคอมพิวเตอร์เกิดการขัดข้องหรือเสียหาย

- ควรใช้วิธีการทางเทคนิคในการเข้ารหัสข้อมูล เพื่อเข้ารหัสข้อมูลสำคัญในเครื่องคอมพิวเตอร์

- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันเครื่องคอมพิวเตอร์มิให้ถูกขโมยหรือสูญหาย ไม่วางเครื่องไว้ในที่สาธารณะหรือบริเวณที่มีความเสี่ยงต่อการสูญหาย

- ห้ามนำเครื่องคอมพิวเตอร์ที่ไม่ใช่ของหน่วยงานมาใช้งานกับเครือข่ายของหน่วยงาน เว้นแต่ได้รับการตรวจสอบจากผู้ดูแลระบบที่เกี่ยวข้องก่อนการใช้งาน

- ห้ามเปลี่ยนแปลงหมายเลขไอพีแอดเดรส (IP Address) ของเครื่องคอมพิวเตอร์ภายในหน่วยงาน

- ต้องทำการสำรองข้อมูลสำคัญที่อยู่ในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ

- ผู้ใช้งานมีหน้าที่รับผิดชอบในการการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกแบบภายนอก หรืออื่น ๆ ที่เหมาะสม

- ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๒) ผู้ใช้งานต้องป้องกันและแก้ไขไวรัสคอมพิวเตอร์หรือซอฟต์แวร์ไม่ประสงค์ดี (Antivirus)

- ตรวจสอบว่าเครื่องคอมพิวเตอร์ที่ใช้งานมีซอฟต์แวร์ป้องกันไวรัส ติดตั้งอยู่และต้องเปิดใช้งานตลอดเวลาที่ใช้งาน

- ปรับปรุงฐานข้อมูลป้องกันไวรัส (Updating Virus Signature Database) ให้เป็นปัจจุบัน

- ห้ามทำการใดเพื่อขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

- ควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จักและจากช่องทางการติดต่อสื่อสาร ที่น่าจะเป็นไปได้เท่านั้น

- ทำการตรวจหาไวรัสทุกครั้งหลังจากรับไฟล์จากแหล่งใด ๆ ก็ตาม มาใช้ที่เครื่องคอมพิวเตอร์

- ใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง โดยไม่เปิดเว็บไซต์เกมส์ออนไลน์ เว็บไซต์ลามกอนาจาร เว็บไซต์ที่ให้ดาวน์โหลดโปรแกรมหรือไฟล์ต่าง ๆ หรือพฤติการณ์อื่นใดที่มีความเสี่ยงต่อการติดไวรัส

- ห้ามติดตั้งโปรแกรม Java, ActiveX หรือโปรแกรมประเภท Active Code อื่นใดจากแหล่งที่ไม่น่าเชื่อถือ

- ไม่เปิดจดหมายอิเล็กทรอนิกส์ (E-Mail) จากบุคคลที่ไม่รู้จักหรือชื่อเรื่องที่ไม่เคยติดต่อกันมาก่อน หรือสงสัยว่าไม่ปลอดภัย

- ไม่เปิดการแบ่งปันข้อมูลแบบ Share Drive หรือหากมีความจำเป็นให้เปิดการแบ่งปันข้อมูลแบบ Share Folder โดยต้องอนุญาตใช้รหัสผ่าน และอนุญาตให้อ่านอย่างเดียว

- ให้ความสำคัญกับการแจ้งเตือนจากซอฟต์แวร์ป้องกันไวรัส หากมีข้อสงสัยหรือพบว่าเครื่องคอมพิวเตอร์ทำงานผิดปกติหรือซอฟต์แวร์ป้องกันไวรัสมีการแจ้งเตือนมากผิดปกติ ให้แจ้งเจ้าหน้าที่ของส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน คู่สัญญาเช่าหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับหน่วยงานเท่านั้น

(๓) การยับยั้งหรือจำกัดความเสียหาย เมื่อเครื่องคอมพิวเตอร์ติดไวรัสคอมพิวเตอร์หรือซอฟต์แวร์ไม่ประสงค์ดี ให้ผู้ที่มีหน้าที่ป้องกันและแก้ไขไวรัสปฏิบัติ ดังนี้

- ให้แยกเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์ผิดปกติออกจากเครือข่ายของหน่วยงาน โดยการถอดสาย LAN หรือปิดอุปกรณ์ไร้สาย (Wireless LAN)

- สำรองข้อมูลสำคัญในเครื่องคอมพิวเตอร์ที่เกิดเหตุการณ์ผิดปกติ

- ให้ทำการตรวจหาไวรัสคอมพิวเตอร์ที่อาจจะฝังตัวอยู่กับข้อมูลที่สำรองไว้ก่อนนำข้อมูลไปใช้กับเครื่องคอมพิวเตอร์อื่น

- ในกรณีที่พบไฟล์ที่ติดไวรัสคอมพิวเตอร์หรือไฟล์ที่เป็นซอฟต์แวร์ไม่ประสงค์ดี และซอฟต์แวร์ป้องกันไวรัสสามารถแก้ไขไวรัสคอมพิวเตอร์ที่ติดได้ ให้ดำเนินการแก้ไขโดยซอฟต์แวร์ป้องกันไวรัส หากซอฟต์แวร์ป้องกันไวรัสไม่สามารถแก้ไขไวรัสคอมพิวเตอร์ที่ติดได้ ให้ลบไฟล์ที่ติดไวรัสคอมพิวเตอร์หรือลบไฟล์ที่เป็นซอฟต์แวร์ไม่ประสงค์ดีทิ้ง

- ให้ติดตั้งโปรแกรมส่วนแก้ไข (Update Patch) ตามความเหมาะสม ปรับปรุงเวอร์ชันซอฟต์แวร์ป้องกันไวรัส และปรับปรุงฐานข้อมูลป้องกันไวรัส (Updating Virus Signature Database) ให้เป็นปัจจุบัน เพื่อเพิ่มประสิทธิภาพในการป้องกันไวรัส

(๔) การจัดทำเอกสารลับบนกระดาษหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

- มีการจัดหมวดหมู่เอกสารลับไว้ต่างหาก และต้องป้องกันให้มีความปลอดภัยอย่างเพียงพอ

- จำกัดการสำเนาเอกสารลับเท่าที่จำเป็นต้องใช้งานเท่านั้น

- ระมัดระวังการกระจาย ส่ง หรือการแจกจ่ายเอกสารลับไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับทราบ หรือใช้งานเอกสารนั้นเท่านั้น

- ใช้วิธีการตามกฎหมายที่หน่วยงานได้ถือปฏิบัติอยู่แล้วสำหรับการจัดส่งเอกสารลับทางไปรษณีย์

(๕) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

(๖) เจ้าของข้อมูลจะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๗) เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลายสื่อหรือข้อมูลอิเล็กทรอนิกส์ ดังนี้

- Flash Drive ใช้วิธีการทุบหรือบดให้เสียหาย

- กระดาษ หรือ แผ่น CD/DVD ใช้วิธีการหั่นด้วยเครื่องทำลายเอกสาร

- เทป ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย

- ฮาร์ดดิสก์ ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แม็ต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหม ประเทศสหรัฐอเมริกา DOD ๕๒๒๐.๒๒-M (ซึ่งเป็นการลบข้อมูลอย่างสมบูรณ์ซึ่งได้รับการยอมรับ โดยทำให้ไม่สามารถกู้ไฟล์กลับคืนมาได้ ซึ่งทำการลบข้อมูล ๓ รอบ รอบแรกด้วยข้อมูลแบบสุ่ม รอบที่สองด้วยบิตที่ตรงกันข้าม รอบสุดท้ายด้วยข้อมูลไบต์สุ่ม)

(๘) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานการรักษาความปลอดภัยของข้อมูลที่รับส่งผ่านอินเทอร์เน็ต (Secure Sockets Layer: SSL) และเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN)

(๙) ผู้ใช้งานอาจนำการเข้ารหัส (Encryption) มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่ม (ฉบับที่ ๒) พ.ศ. ๒๕๖๑

(๑๐) ในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เพื่อส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมหรือจำหน่าย หรือเพื่อการอื่นให้มีการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

(๑๑) ป้องกันไม่ให้บุคคลภายนอกเข้าถึงหรือใช้งานกล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เครื่องโทรสารหรืออุปกรณ์อื่นใดลักษณะเดียวกันนี้ โดยไม่ได้รับอนุญาต

(๑๒) ให้นำเอกสารออกจากเครื่องพิมพ์ เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เครื่องโทรสารหรืออุปกรณ์อื่นใดลักษณะเดียวกันนี้ทันทีที่ใช้งานเสร็จ

(๑๓) ในกรณีที่ต้องการนำสินทรัพย์สารสนเทศต่าง ๆ ออกจากพื้นที่ใช้งาน ต้องขออนุญาตจากผู้บังคับบัญชา

(๑๔) ผู้ใช้งานต้องคืนสินทรัพย์ทั้งหมดที่เกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวพนักงาน บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ เมื่อพ้นการปฏิบัติหน้าที่

(๑๕) ผู้ดูแลระบบต้องระงับสิทธิ หรือถอดถอนสิทธิ หรือเรียกคืนสินทรัพย์ตามเห็นควร หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

(๑๖) การเผยแพร่ข้อมูลข่าวสารบนเว็บไซต์

- ข้อมูลที่จะนำขึ้นเว็บไซต์ ต้องไม่ก่อให้เกิดความเสียหาย ละเมิดสิทธิ หรือสร้างความรำคาญแก่ผู้อื่น หรือผิดกฎหมาย หรือขัดต่อศีลธรรมอันดีของประชาชน

- ในการนำข้อมูลขึ้นเว็บไซต์ ให้ใช้แบบฟอร์มตามที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนกำหนด ซึ่งลงนาม โดยผู้บังคับบัญชาระดับผู้อำนวยการส่วนหรือเทียบเท่า

- ข้อมูลที่จะนำขึ้นเว็บไซต์ ต้องได้รับความเห็นชอบจากผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนหรือผู้ที่ได้รับมอบหมาย

- ให้ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน พิจารณากำหนดระยะเวลาการเผยแพร่ข้อมูลตามความเหมาะสมของข้อมูลที่ต้องเผยแพร่

๕. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ให้ปฏิบัติดังนี้

๕.๑ การใช้บริการเครือข่าย กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) มีการกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้มีการใช้งานได้

(๒) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) มีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้ ดังนี้

(๑) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องยืนยันตัวตน (Identification) ด้วยชื่อผู้ใช้ (Username) ทุกครั้ง

(๒) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ด (Smart Card) เป็นต้น

(๓) การใช้งานระบบสารสนเทศของหน่วยงานผ่านอินเทอร์เน็ต ต้องมีการเข้ารหัสที่เป็นมาตรฐานสากล เพื่อความมั่นคงปลอดภัยด้วยเครือข่ายส่วนตัวเสมือน (Virtual Private Network: VPN)

(๔) การเข้าสู่ระบบสารสนเทศของหน่วยงานผ่านอินเทอร์เน็ต ต้องได้รับอนุญาตจากส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

๕.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) มีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๑) ระบุหมายเลขอุปกรณ์บนเครือข่าย ประกอบด้วย หมายเลขเทอร์มินัล หมายเลขไอพีแอดเดรส (IP Address) และ MAC Address

(๒) ผู้ดูแลระบบจัดทำบัญชีเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่เชื่อมต่อกับเครือข่าย ได้แก่ รายละเอียดเครื่องคอมพิวเตอร์ หมายเลขไอพีแอดเดรส (IP Address) MAC Address สถานที่ติดตั้งและชื่อผู้ใช้งาน

(๓) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนหรือผู้ที่ได้รับอนุญาตเท่านั้น

(๔) ต้องใช้ไฟร์วอลล์ (Firewall) กำหนดหมายเลขอุปกรณ์ ที่สามารถเข้าถึงเครือข่ายของหน่วยงานได้

(๕) จัดทำแผนผังระบบเครือข่าย ประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก โดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย

(๖) ทำการทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันเสมอ อย่างน้อยปีละ ๑ ครับ

๕.๔ การป้องกันพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ดังนี้

(๑) การเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่ายต้องมีการตั้งรหัสผ่าน (Password) และให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(๒) มีการป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่ายและเปิดเฉพาะอุปกรณ์และเวลาที่จำเป็นเท่านั้น

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

(๔) ทำการติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

๕.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่าย โดยให้แยกเป็น

(๑) Management Zone เป็นระบบเครือข่ายที่ใช้ในการควบคุมการบริหารจัดการระบบคอมพิวเตอร์และเครือข่าย

(๒) Demilitarized Zone เป็นระบบคอมพิวเตอร์และเครือข่ายที่ให้บริการข้อมูลข่าวสารทั้งภายในหน่วยงาน (Intranet Zone) และภายนอกหน่วยงาน (Extranet Zone)

(๓) Intranet Zone เป็นระบบเครือข่ายภายในหน่วยงาน สำหรับการใช้งานข้อมูลสารสนเทศที่มีความสำคัญและเข้าถึงได้เฉพาะบุคลากรของหน่วยงานที่ได้รับอนุญาตเท่านั้น

(๔) Extranet Zone เป็นระบบเครือข่ายเชื่อมต่อกับภายนอกหน่วยงานสำหรับการรับ-ส่งข้อมูลกับหน่วยงานภายนอก

๕.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

(๑) จำกัดสิทธิของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

(๒) ระดับเครือข่ายทั้งหมดต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Intrusion Detection System: IDS/Intrusion Prevention System: IPS, ไฟร์วอลล์ (Firewall))

(๓) การเข้าสู่ระบบเครือข่ายของหน่วยงานต้องเข้าสู่ระบบผ่านช่องทางที่ปลอดภัยเพื่อยืนยันตัวตน

(๔) ควบคุมการเชื่อมต่อทางเครือข่ายของผู้ใช้งานตามวันที่ เวลา หรือช่วงเวลาที่อนุญาตให้ใช้งาน

๕.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ดังนี้

(๑) ควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

(๒) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขไอพีแอดเดรส (IP Address)

(๓) กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน (Domain Name) เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก

(๔) ผู้ดูแลระบบต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ เพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

๕.๘ ข้อกำหนดการป้องกันการบุกรุก (Firewall Policy)

(๑) ผู้ดูแลระบบ มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ (Firewall)

(๒) การกำหนดค่าเริ่มต้นพื้นฐานของทุกเครือข่ายจะต้องเป็นการปฏิเสธทั้งหมด

(๓) ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบาย จะต้องถูกบล็อกโดยไฟร์วอลล์ (Firewall)

(๔) ผู้ใช้งานอินเทอร์เน็ตจะต้องมีการลงบันทึกการเข้า (Login) ก่อนการใช้งานทุกครั้ง

(๕) ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ (Firewall) เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการและการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

(๖) การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ (Firewall) จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายเท่านั้น

(๗) ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ (Firewall) จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

(๘) การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่าย จะเปิดพอร์ต (Port) การเชื่อมต่อพื้นฐานของโปรแกรมทั่วไป ที่ทางส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนอนุญาตให้ใช้งาน ซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ต (Port) การเชื่อมต่อนอกเหนือที่กำหนดจะต้องได้รับความยินยอมจากทางส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

(๙) การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่าย จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ต (Port) การเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยจะต้องถูกระบุให้กับเครื่องคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

(๑๐) จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์ (Firewall) เป็นประจำทุกสัปดาห์หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

(๑๑) ค่ารายการการป้องกันการเข้าถึง (Access Control Lists/Firewall Rules) ควรมีการปรับปรุงและทสบทวนให้สอดคล้องกับสถานภาพปัจจุบันด้านเทคโนโลยีสารสนเทศ หรือเมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

(๑๒) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

(๑๓) ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมีสิทธิที่จะระงับหรือบล็อกการใช้งานเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีการเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

(๑๔) การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการ ตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

(๑๕) ผู้ละเมิดนโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall) จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

๕.๙ ข้อกำหนดการตรวจจับการบุกรุก (IDS/IPS Policy)

(๑) กำหนดให้มีการบันทึกและการบริหารจัดการข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นไปตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์และที่เกี่ยวข้อง เพื่อใช้เป็นข้อมูลสำหรับการตรวจจับการบุกรุก

(๒) ต้องมีการเฝ้าตรวจสอบหรือเรียนรู้พฤติกรรมที่อาจเป็นความเสี่ยงหรือส่งผลกระทบต่อระบบสารสนเทศและเครือข่ายที่มีอยู่ของหน่วยงาน และสามารถยับยั้งการทำงานนั้นได้ทันที โดยในกรณีที่ตรวจสอบและพบว่ามีเหตุการณ์ของการบุกรุกและโจมตี จะต้องกำหนดวิธีการปฏิบัติหรือกิจกรรม และมีผู้รับผิดชอบที่ชัดเจนในการแก้ไขหรือปรับปรุงเหตุการณ์ดังกล่าว

(๓) ระบบตรวจจับการบุกรุกระบบเครือข่าย จะต้องกำหนดให้มีการป้องกันการบุกรุกและโจมตีจากเครือข่ายภายนอก โดยการเรียนรู้พฤติกรรมการบุกรุกและโจมตีระบบ

(๔) ระบบตรวจจับการบุกรุกระบบเครือข่าย จะต้องกำหนดให้มีการปรับปรุงการกำหนดค่าด้านความมั่นคงปลอดภัยที่สามารถเรียนรู้พฤติกรรมการบุกรุกและโจมตี เพื่อให้สามารถเรียนรู้พฤติกรรมการบุกรุกและโจมตีระบบรูปแบบใหม่ ๆ ได้

(๕) ระบบตรวจจับการบุกรุกระบบเครือข่าย จะต้องกำหนดให้มีมาตรการในการป้องกันการโจมตีการทำงานของระบบตรวจจับการบุกรุกระบบเครือข่ายไม่ให้ทำงานผิดพลาด โดยต้องไม่เปิดเผยให้สามารถตรวจสอบหมายเลขไอพีแอดเดรส (IP Address) หรือเส้นทาง (Path) ในระบบเครือข่าย หรือมาตรการอื่นใดในการป้องกันการโจมตี ทั้งนี้ให้มีการตรวจสอบและทบทวนมาตรการให้มีความสอดคล้องกับสถานภาพด้านเครือข่ายในปัจจุบัน อย่างน้องปีละ ๒ ครั้ง หรือมีการเปลี่ยนแปลงสถานภาพด้านเครือข่ายที่มีผลกระทบ

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ให้ดำเนินการ ดังนี้

๖.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องมีการยืนยันตัวตนที่มีความมั่นคงปลอดภัย ดังนี้

(๑) ต้องไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๓) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๖.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง ดังนี้

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(๒) หากอนุญาตให้ใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านด้านเทคนิค หรือความสอดคล้องกับการปฏิบัติงาน

(๓) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น สมาร์ทการ์ด (Smart Card)

๖.๓ การบริหารจัดการรหัสผ่าน (Password Management System) ดังนี้

(๑) ให้มีการใช้เทคนิคการตรวจสอบการกำหนดรหัสผ่านซึ่งประกอบด้วยอักขระ ตัวเลข และอักขระพิเศษ หรือเทคนิคอื่นใดในการบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๒) เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๖.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ดังนี้

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ที่ไม่ได้ใช้งานเป็นประจำไว้ในสื่อภายนอก

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) ให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๖) ห้ามติดตั้งหรือใช้งานโปรแกรมละเมิดลิขสิทธิ์หรือโปรแกรมที่มีนโยบายห้ามไม่ให้เข้าถึงหรือติดตั้งหรือใช้งาน รวมไปถึงใช้วิธีการในการหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดหรือที่มีอยู่แล้วด้วย

(๗) หน่วยงานไม่สนับสนุนการติดตั้งและ/หรือใช้งานโปรแกรมละเมิดลิขสิทธิ์ หากเกิดข้อพิพาทผู้ที่ติดตั้งและ/หรือใช้งานโปรแกรมดังกล่าวต้องเป็นผู้รับผิดชอบ

๖.๕ การกำหนดเวลาเพื่อยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน (Session Tine-Out) ดังนี้

(๑) กำหนดให้ระบบสารสนเทศมีการตัดและหมดเวลาการใช้งานรวมถึงปิดการใช้งานหลังจากที่ว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาที

(๒) ระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง ต้องมีการตัดและหมดเวลาในการใช้งานที่สั้นขึ้น เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๖.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ดังนี้

(๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชัน (Application) ที่มีความเสี่ยงหรือมีความสำคัญสูง แต่ละครั้งไม่เกิน ๓ ชั่วโมง โดยจะต้องระบุและพิสูจน์ยืนยันตัวตนเพื่อเข้าใช้งานใหม่

(๒) กำหนดให้ระบบระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง มีการจำกัดช่วงระยะเวลาการเชื่อมต่อให้ใช้งานได้เฉพาะช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น และมีการจำกัดระยะเวลาการเชื่อมต่อที่สั้นขึ้น

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

ต้องมีการควบคุม ดังนี้

๗.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ดังนี้

(๑) ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของหน่วยงาน ตามข้อกำหนดการลงทะเบียนผู้ใช้งานและการบริหารจัดการสิทธิของผู้ใช้งาน เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบสารสนเทศและข้อมูลต่าง ๆ

(๒) ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่าง ๆ และหากไม่มีการใช้งานนานเกินระยะเวลาที่กำหนด ต้องยกเลิกการเชื่อมต่อระบบ

(๓) ผู้ให้บริการภายนอก (Outsource) ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของหน่วยงาน

(๔) ผู้ดูแลระบบต้องดำเนินการเพิกถอนหรือเปลี่ยนแปลงสิทธิการเข้าถึงระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ที่สิ้นสุดการว่าจ้างโดยทันที

(๕) ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลของผู้ให้บริการภายนอก (Outsource) ให้มีสิทธิเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง และตรวจสอบการนำข้อมูลเข้าและออกจากระบบสารสนเทศของผู้ให้บริการภายนอก (Outsource) ทุกครั้ง

๗.๒ การบริหารจัดการระบบซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ดังนี้

(๑) ต้องมีการระบุความสำคัญของระบบงานซึ่งไวต่อการรบกวน หรือมีผลกระทบสูงต่อหน่วยงาน

(๒) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อหน่วยงาน

(๓) ต้องมีการประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกัน ระหว่างระบบงานที่มีความสำคัญสูงกับระบบงานอื่น ๆ ที่มีความสำคัญน้อยกว่า

(๔) ต้องมีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

(๕) ต้องมีการสำรองและทดสอบการกู้คืนระบบ ตามนโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

(๖) ต้องมีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๗.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ (Mobile Computing) เพื่อควบคุมการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต จากการเสียหาย สูญหาย ถูกขโมย ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

- การป้องกันอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ครอบคลุมการใช้งานอุปกรณ์สื่อสารแบบพกพาประเภทโทรศัพท์มือถือ สมาร์ทโฟน (Smartphone) เครื่องช่วยงานส่วนบุคคลแบบดิจิทัล (Personal Digital Assistants: PDA) โน้ตบุ๊ก (Notebook) แล็ปท็อป (Laptop) แท็บเล็ต (Tablet) หรืออุปกรณ์อื่นใดลักษณะเดียวกันนี้
- ต้องกำหนดรหัสผ่านที่มีความมั่นคงปลอดภัยสำหรับผู้ใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่
- ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือลับในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่
- ให้ใช้วิธีการทางเทคนิคในการเข้ารหัสข้อมูล เพื่อเข้ารหัสข้อมูลสำคัญในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่
- เมื่อพบซอฟต์แวร์ไม่ประสงค์ดีในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ให้ปฏิบัติตามข้อปฏิบัติในการป้องกันซอฟต์แวร์ไม่ประสงค์ดีและที่เกี่ยวข้อง
- ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ มิให้ถูกขโมยหรือสูญหาย โดยการล็อกเครื่องขณะไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหายโดยทำการล็อกอุปกรณ์ไว้กับโต๊ะ หรือนำไปเก็บไว้ในที่ตู้ที่สามารถล็อกได้ หรือวิธีการอื่นใดที่เหมาะสม
- ให้ทำการสำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่อย่างสม่ำเสมอ
- กำหนดให้มีการป้องกันการเชื่อมต่ออุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่เข้ากับเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาต
- ให้ใส่ซองกันกระแทกหรือกระเป๋าสำหรับอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือนจากการตกหล่น หรือพฤติกรรมอื่นใด
- ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่
- ให้ติดตั้งหรือจัดเก็บอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่บนโต๊ะ ชั้นวางของหรือสิ่งอื่นใดที่เป็นอุปกรณ์เฉพาะสำหรับติดตั้งหรือเก็บรักษาที่มั่นคงแข็งแรง
- เพื่อความเป็นระเบียบและปลอดภัยสำหรับอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ให้จัดเก็บสายชาร์ต สายเชื่อมต่อกับระบบคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องอื่นใด ไว้ในสถานที่หรืออุปกรณ์เฉพาะที่สามารถปิดล็อกได้เพื่อป้องกันการสูญหาย
- ตรวจสอบสายสัญญาณของอุปกรณ์ สายชาร์ต สายเชื่อมต่อกับระบบคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องอื่นใดให้เรียบร้อย เพื่อความเป็นระเบียบและป้องกันอุบัติเหตุที่อาจทำให้อุปกรณ์สื่อสารได้รับความเสียหาย
- ทำความสะอาดอุปกรณ์สื่อสารอย่างสม่ำเสมอ เพื่อป้องกันฝุ่นละอองที่จะทำให้อุปกรณ์สื่อสารเกิดการขัดข้องเสียหาย

(๒) การควบคุมการติดตั้งระบบหรืออุปกรณ์ต่าง ๆ เพิ่มเติม

- ห้ามติดตั้งโปรแกรมเพิ่มเติมนอกเหนือจากที่หน่วยงานได้ติดตั้งไว้ให้ใช้งาน
- ห้ามติดตั้งโปรแกรมที่สามารถตรวจสอบข้อมูลบนระบบเครือข่าย ยกเว้นติดตั้งเพื่อปฏิบัติงานของผู้ดูแลระบบที่เกี่ยวข้อง
- ห้ามติดตั้งโปรแกรมหรืออุปกรณ์อื่นใดเพิ่มเติม เพื่อให้บุคคลอื่นสามารถใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ หรือเครือข่ายของหน่วยงานได้
- ห้ามนำอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ที่ไม่ใช่ของหน่วยงานมาใช้กับเครือข่ายหน่วยงาน เว้นแต่ได้รับการตรวจสอบความปลอดภัยและตั้งค่าการใช้งานจากผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้องก่อนการใช้งาน

(๓) ข้อกำหนดในการสำรองข้อมูลและการกู้คืน

- ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกประเภท CD, DVD, External Hard Disk หรือสื่อบันทึกอื่นใดที่เหมาะสม ในการใช้สำรองข้อมูลจากเครื่องคอมพิวเตอร์
- ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๗.๔ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) เพื่อป้องกันการใช้งานระบบสารสนเทศโดยไม่ได้รับอนุญาตจากการปฏิบัติงานจากภายนอกหน่วยงาน ให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) ให้มีการเข้ารหัส (Encryption) ด้วย SSL VPN, XML Encryption หรือวิธีการอื่นใดที่เป็นมาตรฐานสากล ในการสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากภายนอกหน่วยงานและระบบงานต่าง ๆ ภายในหน่วยงาน ทั้งนี้ให้มีความเหมาะสมกับรูปแบบการสื่อสารของความสำคัญของข้อมูล

(๒) การเข้าถึงระบบสารสนเทศของหน่วยงานจากระยะไกลด้วยอุปกรณ์ที่เป็นของส่วนตัว ต้องได้รับอนุญาตจากส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

(๓) การเปิดใช้งานระบบสารสนเทศให้สามารถปฏิบัติงานจากภายนอกหน่วยงานได้ ต้องมีหนังสือเป็นลายลักษณ์อักษรและมีความเห็นชอบของผู้บังคับบัญชาตามลำดับชั้น และได้รับความเห็นชอบจากผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน โดยระบุรายละเอียดดังนี้

- เหตุผลความจำเป็นที่ต้องการให้สามารถปฏิบัติงานจากภายนอกหน่วยงาน
- รายละเอียดและ/หรือลักษณะของระบบงาน
- ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอก
- รายชื่อผู้ใช้งาน หรือกลุ่มผู้ใช้งาน
- ช่วงเวลาและระยะเวลาในการใช้ปฏิบัติงานจากภายนอกหน่วยงาน

(๔) ไม่อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานสำหรับระบบงานที่มีความลับชั้นลับ ชั้นลับมาก และชั้นลับมากที่สุด

(๕) ให้ผู้ที่ได้รับอนุญาตเท่านั้นสามารถเข้าถึงระบบสารสนเทศและข้อมูลของหน่วยงาน โดยห้ามมิให้สมาชิกในครอบครัวหรือบุคคลใด ๆ ที่ไม่ได้รับอนุญาต และขอสงวนสิทธิในการระงับหรือยกเลิกสิทธิหากพบว่าไม่ปฏิบัติตามนโยบายและระเบียบปฏิบัติที่เกี่ยวข้อง

(๖) การยกเลิกสิทธิในการปฏิบัติงานจากภายนอกหน่วยงาน ให้มีหนังสือเป็นลายลักษณ์อักษรขอยกเลิกต่อผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน ทันทีที่ครบระยะเวลาหรือเมื่อหมดความจำเป็นในการใช้ปฏิบัติงานจากภายนอกหน่วยงาน

(๗) ให้มีการทบทวนปรับปรุงสิทธิการอนุญาตให้ใช้ปฏิบัติงานจากภายนอกหน่วยงานอย่างน้อยปีละ ๑ ครั้ง

๘. การควบคุมการเข้าถึงเครือข่ายไร้สาย (Wireless LAN Access Control)

๘.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการส่วนหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๘.๒ ผู้ดูแลระบบ (System Administrator) ต้องดำเนินการดังนี้

(๑) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๒) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๓) ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

(๔) ต้องเปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

(๕) ต้องกำหนดค่าใช้ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากที่สุด

(๖) ต้องเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น

(๗) ต้องมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

(๘) ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนทราบโดยทันที

๘.๓ ข้อกำหนดในการขอใช้เครือข่ายไร้สาย

(๑) เป็นบุคลากรในสังกัดสำนักบริหารการทะเบียน จะต้องได้รับการพิจารณาจากผู้บังคับบัญชาระดับผู้อำนวยการส่วนหรือเทียบเท่า

(๒) ผู้ขอใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของหน่วยงาน ต้องทำการลงทะเบียนกับส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน และต้องได้รับอนุญาตจากผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนอย่างเป็นลายลักษณ์อักษรทุกครั้ง

(๓) ห้ามผู้ใช้งานติดตั้งอุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) โดยไม่ได้รับอนุญาต

(๔) การใช้บริการทางอินเทอร์เน็ต ให้ปฏิบัติตามข้อ ๑๒. การใช้งานระบบอินเทอร์เน็ต (Internet)

๘.๔ ขั้นตอนการขอใช้เครือข่ายไร้สาย

(๑) ผู้ขอใช้งาน ต้องมีคุณสมบัติตามข้อกำหนดในการขอใช้เครือข่ายไร้สาย

(๒) ผู้ขอใช้งาน ต้องกรอกรายละเอียดลงในแบบขอใช้งานเครือข่ายไร้สายที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนกำหนด พร้อมทั้งให้ผู้บังคับบัญชาลงนามรับรอง

(๓) เมื่อส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนได้รับหนังสือ ผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนพิจารณาอนุมัติ ให้ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายดำเนินการต่อไป

(๔) ในกรณีที่ผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนพิจารณาไม่อนุมัติ ให้มีหนังสือแจ้งเหตุผลของการไม่อนุมัติกลับไปยังต้นเรื่อง

(๕) ผู้ดูแลระบบสามารถระงับหรือยกเลิกสิทธิการใช้เครือข่ายไร้สายได้ทันที เมื่อพบว่าผู้ใช้งานมีการกระทำเข้าข่ายไม่ปฏิบัติตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

เพื่อให้มีการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายอย่างเหมาะสม ไม่ก่อให้เกิดความเสี่ยงในการเข้าถึงระบบสารสนเทศและเครือข่ายของหน่วยงานโดยไม่ได้รับอนุญาต และให้เครื่องคอมพิวเตอร์แม่ข่ายทำงานได้อย่างมีประสิทธิภาพ มีความถูกต้อง น่าเชื่อถือ และพร้อมใช้งานให้ปฏิบัติ ดังนี้

๙.๑ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(๑) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงานเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

(๒) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของหน่วยงาน

(๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ที่อาจกระทบต่อการให้บริการของระบบสารสนเทศต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

(๔) ไม่ติดตั้งซอร์สโค้ด (Source Code) คอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

(๕) ให้มีการจัดเก็บซอร์สโค้ด (Source Code) และไลบรารี่ (Library) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๖) ให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ หรือซอฟต์แวร์หรือระบบสารสนเทศอื่นใด ตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(๗) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

(๘) ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้นตามระยะเวลาที่เหมาะสม

(๙) ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

๙.๒ ข้อกำหนดในการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบ และทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๙.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

(๑) ให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

(๒) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในสินทรัพย์ทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบซอฟต์แวร์ไม่ประสงค์ดี ในซอฟต์แวร์ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๙.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค

(๑) ให้มีการจัดทำบัญชีของระบบสารสนเทศ เพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟแวร์นั้น ๆ

(๒) ให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

(๓) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบการดำเนินการดังนี้

- มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
- ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน
- ให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

(๔) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๙.๔ ข้อกำหนดในการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) และการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ข้อมูลชื่อผู้ใช้งาน

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ

(๓) ข้อมูลวันเวลาที่ออกจากระบบ

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๕) ข้อมูลการลงบันทึกการเข้า (Login) ทั้งที่สำเร็จและไม่สำเร็จ

(๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๗) ข้อมูลการเปลี่ยนการกำหนดค่า (Configuration) ของระบบ

(๘) ข้อมูลแสดงการใช้งานแอปพลิเคชัน (Application)

(๙) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์ เป็นต้น

(๑๐) ข้อมูลหมายเลขไอพีแอดเดรส (IP Address) ที่เข้าถึง

(๑๑) ข้อมูลโปรโตคอลเครือข่าย (Network Protocol) ที่ใช้

(๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

(๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๑๐. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

เพื่อรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม ไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต

๑๐.๑ การรักษาความมั่นคงปลอดภัยห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร มีดังนี้

(๑) พื้นที่ใช้งานระบบสารสนเทศและการสื่อสารแบ่งออกเป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย และพื้นที่สำหรับผู้มาติดต่อ

(๒) จัดทำแผนผังพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

(๓) กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

(๔) การควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ให้ปฏิบัติตามข้อ ๑๔. การใช้ห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

(๕) หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

(๖) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังนี้ เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบน้ำ ระบบดับเพลิง ระบบปรับอากาศ ระบบควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านี้อย่างสม่ำเสมอ

(๗) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

(๘) เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูงต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก และสำนักงานหรือห้องจะต้องมีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๙) เจ้าหน้าที่ผู้ได้รับมอบหมายต้องตรวจสอบความมั่นคงปลอดภัยของพื้นที่ที่ตนได้รับมอบหมายเป็นประจำ เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก อุปกรณ์ต่าง ๆ สื่อบันทึกข้อมูลที่สำคัญถูกจัดเก็บหรือได้รับการปิดล็อกอย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๑๐.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security) มีดังนี้

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ให้มีการป้องกันการเข้าถึงจากบุคคลภายนอก

(๗) พิจารณาใช้งานสายไฟเบอร์ออฟติก (Fiber Optic) แทนสายสัญญาณสื่อสารแบบเดิมสำหรับระบบสารสนเทศที่สำคัญ

(๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๑๐.๓ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance) มีดังนี้

(๑) ให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ให้ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

(๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑๐.๔ การนำสินทรัพย์ของหน่วยงานออกนอกหน่วยงาน (Removal of Property) มีดังนี้

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือสินทรัพย์นั้นออกไปใช้งานนอกหน่วยงาน

(๒) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้ง บันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๑๐.๕ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment Off-Premises) มีดังนี้

(๑) ให้มีการป้องกันอุปกรณ์มิให้โดนกระแทก แตกหักในระหว่างการขนส่งหรือเคลื่อนย้าย

(๒) ไม่ทิ้งอุปกรณ์หรือสินทรัพย์ของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์เสมือนเป็นสินทรัพย์ของตนเอง

๑๐.๖ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-Use of Equipment) มีดังนี้

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) ให้มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้น

๑๐.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ มีดังนี้

(๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

(๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ

๑๑. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๑.๑ ขั้นตอนการขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

(๑) ผู้ขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องเป็นบุคลากรสังกัดในหน่วยงาน

(๒) ผู้ขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ดาวน์โหลดหรือรับแบบฟอร์มการขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ของหน่วยงาน

(๓) ผู้ขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) กรอกข้อมูลลงในแบบฟอร์มฯ ให้ครบถ้วน และให้ผู้บังคับบัญชาระดับผู้อำนวยการส่วนหรือเทียบเท่าให้ความเห็นชอบ

(๔) มีหนังสือขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) พร้อมแนบแบบฟอร์มฯ ถึงผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

(๕) เมื่อได้รับการอนุมัติ ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนจะทำการส่งชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) กลับไปให้ผู้ขอใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๑.๒ การใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

(๑) ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ทั้งหมดของหน่วยงาน ต้องมีบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) เป็นของตนเอง

(๒) ผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องเปลี่ยนรหัสผ่าน (Password) ทันทีหลังจากการเข้าสู่ระบบเป็นครั้งแรก

(๓) บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ต้องได้รับการปกป้องด้วยรหัสผ่าน (Password) เพื่อป้องกันการถูกล่วงละเมิดและการนำไปใช้ในทางที่ผิด

(๔) บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ที่มีวัตถุประสงค์พิเศษ เช่น webmaster@bora.dopa.go.th ที่สร้างขึ้นเพื่อเป็นบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) กลางของส่วนงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) นั้น

(๕) บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ทั้งหมด และจดหมายอิเล็กทรอนิกส์ (E-Mail) ทุกฉบับ (รวมถึงจดหมายอิเล็กทรอนิกส์ (E-Mail) ส่วนตัว) ที่ถูกสร้างและเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของหน่วยงาน ถือเป็นสินทรัพย์ของหน่วยงาน

(๖) ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือ ติดต่อสื่อสารกับระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) ของหน่วยงาน

(๗) พื้นที่เก็บจดหมายอิเล็กทรอนิกส์ (E-Mail) บนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้เมื่อปริมาณจดหมายอิเล็กทรอนิกส์ (E-Mail) มากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบ

(๘) ต้องใช้บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ของหน่วยงานเพื่อติดต่องานของราชการเท่านั้น ห้ามใช้เพื่อการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย

(๙) ห้ามใช้บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ของหน่วยงานในการประกาศข้อมูลใด ๆ ในเว็บบอร์ด บล็อก กระดานข่าว หรือสื่อสังคมออนไลน์อื่นใด เว้นแต่การประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการทำงานให้กับหน่วยงาน

(๑๐) ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในจดหมายอิเล็กทรอนิกส์ (E-Mail) หัวจดหมายอิเล็กทรอนิกส์ (E-Mail) ลายเซ็นในจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ของบุคคลอื่นโดยเด็ดขาด

(๑๑) การแจ้งที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของหน่วยงานให้บุคคลอื่นให้ใช้เพื่อการผลประโยชน์ทางราชการ

(๑๒) ห้ามใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ของหน่วยงานในการติดต่อเรื่องส่วนตัวกับบุคคลหรือหน่วยงานที่ไม่รู้จักหรือไม่น่าเชื่อถือ

(๑๓) ขอสงวนสิทธิในการเพิกถอนสิทธิการใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) หากพบว่าจดหมายอิเล็กทรอนิกส์ (E-Mail) ดังกล่าวถูกนำไปใช้งานขัดต่อนโยบายของหน่วยงาน ระเบียบปฏิบัติ หรือกฎหมายที่เกี่ยวข้อง

๑๑.๓ การส่งจดหมายอิเล็กทรอนิกส์ (E-Mail)

(๑) ห้ามผู้ใช้งานส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อหน่วยงาน

(๒) ซอฟต์แวร์สำหรับใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องได้รับการตั้งค่าให้จดหมายอิเล็กทรอนิกส์ (E-Mail) ส่งออกทุกฉบับมีลายเซ็นของผู้ส่งเสมอ โดยลายเซ็นนั้นต้องประกอบด้วย ชื่อ-นามสกุล ตำแหน่ง ชื่อหน่วยงานและเบอร์โทรศัพท์ติดต่อ

(๓) ห้ามผู้ใช้งานส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีเนื้อหาหรือรูปภาพที่เข้าข่ายดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศหรือจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรมหรือศาสนาและจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีผลกระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

(๔) ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) หลอกลวงหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ในลักษณะลูกโซ่โดยเด็ดขาด

(๕) ห้ามผู้ใช้งานส่งจดหมายอิเล็กทรอนิกส์ขยะ (Junk Mail) โฆษณาสินค้าต่าง ๆ (Spam Mail) หรือจดหมายอิเล็กทรอนิกส์ (E-Mail) อื่นใดที่ผู้รับไม่ได้ต้องการ

(๖) ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) โดยใช้บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Account) ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใด ก็ตาม

(๗) ผู้ใช้งานต้องร่างเนื้อหาของจดหมายอิเล็กทรอนิกส์ (E-Mail) ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกจดหมายอิเล็กทรอนิกส์ (E-Mail) นั้นในนามตัวแทนของหน่วยงาน

(๘) ไฟล์เอกสารที่แนบมาพร้อมกับจดหมายอิเล็กทรอนิกส์ (E-Mail) จะต้องอยู่ในรูปแบบ .pdf, .doc, .xls, .ppt, .txt, csv, jpg, gif, html หรือในรูปแบบตามมาตรฐานอื่นใด ซึ่งผู้รับสามารถเปิดอ่านได้ด้วยซอฟต์แวร์พื้นฐานบนทุกระบบปฏิบัติการ

(๙) ห้ามส่งข้อมูลลับแนบกับจดหมายอิเล็กทรอนิกส์ (E-Mail) เว้นแต่กรณีที่มีความจำเป็นซึ่งต้องเข้ารหัสก่อน

(๑๐) การส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่มีไฟล์แนบขนาดใหญ่เกิน ๑๐ MB ควรบีบอัดไฟล์แนบให้เล็กลงก่อนส่ง และหากจดหมายอิเล็กทรอนิกส์ (E-Mail) ดังกล่าวไม่เกี่ยวข้องกับงาน ให้ส่งนอกเวลาราชการ

๑๑.๔ การรับจดหมายอิเล็กทรอนิกส์ (E-Mail)

(๑) เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ป้องกันไวรัสว่า เครื่องคอมพิวเตอร์ของตนมีไวรัส ผู้ใช้งานต้องระงับการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) โดยทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

(๒) ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัสจดหมายอิเล็กทรอนิกส์ (E-Mail) บอมม์ หรือซอฟต์แวร์ไม่ประสงค์ดีต่าง ๆ

(๓) ผู้ใช้งานต้องลบจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่จำเป็นออกจากกล่องจดหมาย (Mailbox) ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บจดหมายอิเล็กทรอนิกส์ (E-Mail) ให้เป็นไปตามขนาดที่หน่วยงานกำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่เกี่ยวข้องกับการทำงาน และจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่ขัดต่อกฎหมายเท่านั้น

(๔) ไม่ควรเปิดไฟล์แนบสกุล .exe, .com, .bat หรือไฟล์ประเภทโปรแกรมกระทำการอื่นใดที่ไม่เกี่ยวข้องกับงาน

(๕) ในกรณีที่ได้รับจดหมายอิเล็กทรอนิกส์ (E-Mail) ฉบับเดียวกันซ้ำหลายครั้งหรือได้รับจดหมายอิเล็กทรอนิกส์ (E-Mail) จากบุคคลที่ไม่รู้จักเป็นประจำ หรือลักษณะอื่นใดที่สงสัยว่ามีการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ผิดปกติขึ้น ให้รีบแจ้งส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนดำเนินการตรวจสอบ

๑๑.๕ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ (System Administrator)

(๑) กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน

(๒) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๖ ครั้ง

(๓) มีการทบทวนสิทธิการเข้าใช้งานและปรับปรุงบัญชีผู้ใช้ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น ลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(๔) มีการควบคุมการเข้าถึงระบบตามแนวปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้อย่างเคร่งครัด

๑๒. การใช้งานระบบอินเทอร์เน็ต (Internet)

๑๒.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบอินเทอร์เน็ตจะต้องทำการลงทะเบียนผู้ใช้งาน

๑๒.๒ ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้หน่วยงาน และบุคคลผู้ที่เกี่ยวข้องกับหน่วยงาน เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือว่าเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

๑๒.๓ การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่านทางช่องทาง (Gateway) ที่ได้รับอนุญาตหรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้ หน่วยงานขอสงวนสิทธิในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม

๑๒.๔ ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบ Pop-up หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม (Spam) เนื่องจากเว็บไซต์เหล่านี้อาจมีซอฟต์แวร์ไม่ประสงค์ดีแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

๑๒.๕ ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย

๑๒.๖ หน่วยงานไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวผ่านทางเว็บบอร์ด บล็อก หรือสื่อสังคมออนไลน์อื่นใด ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจาการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของผู้นั้น

๑๒.๗ ห้ามผู้ใช้งานติดตั้งซอฟต์แวร์จากเว็บไซต์ หรือแหล่งข้อมูลที่ไม่น่าเชื่อถือหรือไม่ปลอดภัยต่อระบบสารสนเทศ เว้นแต่ในกรณีที่มีความจำเป็นให้แจ้งส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน เพื่อพิจารณาความปลอดภัยและความเหมาะสม

๑๒.๘ กรณีที่มีความจำเป็นต้องดาวน์โหลดข้อมูลหรือไฟล์ขนาดใหญ่เกิน ๑๐ MB ผ่านอินเทอร์เน็ต ควรกระทำนอกเวลาราชการ เพื่อป้องกันผลกระทบต่อปริมาณข้อมูลในเครือข่าย

๑๒.๙ ตรวจสอบไวรัสในข้อมูลหรือไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ตทุกครั้ง ก่อนติดตั้งหรือใช้งาน

๑๒.๑๐ ผู้ใช้งานมีหน้าที่ระมัดระวังการใช้งาน และต้องรับผิดชอบต่องานหรือผลที่เกิดจากการเรียกใช้บริการบนอินเทอร์เน็ตดังต่อไปนี้

(๑) ไม่ใช้เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายต่อสิทธิ เสรีภาพหรือสินทรัพย์ของผู้อื่น

(๒) ไม่ใช้เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

(๓) ไม่ใช้เพื่อการกระทำอันเป็นการละเมิดเข้าถึงข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาต

(๔) ไม่ใช้เพื่อการกระทำอันมีลักษณะเป็นการละเมิดสินทรัพย์ทางปัญญาของหน่วยงานหรือของบุคคลอื่น

(๕) ไม่ใช่เพื่อการค้า หรือผลประโยชน์ทางธุรกิจ

(๖) ไม่ใช้เพื่อเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงานให้แก่หน่วยงาน ไม่ว่าจะเป็นข้อมูลของหน่วยงาน หรือบุคคลภายนอกก็ตาม

(๗) ไม่ใช้เพื่อรบกวน หรือขัดขวางการใช้งานระบบเครือข่ายคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์ ทั้งในและนอกหน่วยงาน ไม่ให้สามารถใช้งานได้ตามปกติ

(๘) ไม่ใช้เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของหน่วยงาน ไปยังที่เว็บไซต์ใด ๆ ในลักษณะที่จะก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง หรือก่อให้เกิดความขัดแย้งในสังคม

(๙) ไม่ใช้เพื่อการอื่นใดที่อาจก่อให้เกิดความเสียหายแก่หน่วยงาน

๑๒.๑๑ ผู้ดูแลระบบสามารถระงับหรือยกเลิกสิทธิในการเรียกใช้บริการบนอินเทอร์เน็ตได้ทันที เมื่อพบว่าผู้ใช้งานมีการกระทำเข้าข่ายไม่ปฏิบัติตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๑๓. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๓.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่หน่วยงานได้กำหนดไว้เท่านั้น

๑๓.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัยอยู่เสมอและต้องรับผิดชอบหากเกิดความเสียหายใด ๆ ที่มีผลกระทบกับหน่วยงานจากการใช้งานเครือข่ายสังคมออนไลน์

๑๓.๓ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับหน่วยงาน ผู้ใช้งานต้องแจ้งต่อส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๔. การใช้ห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

เพื่อควบคุมการเข้าถึงทางกายภาพและป้องกันสินทรัพย์จากการสูญหาย เสียหาย รวมถึงการเข้าถึงระบบโดยไม่ได้รับอนุญาต ผู้ที่สามารถเข้าห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารได้ ต้องเป็นผู้ที่ได้รับอนุญาตเท่านั้น

๑๔.๑ การขออนุญาตเข้าปฏิบัติงานห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

(๑) หน่วยงานที่ขอเข้าปฏิบัติงานต้องทำหนังสือขออนุญาตเพื่อให้ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนเป็นผู้พิจารณาอนุญาต ได้แก่

- หน่วยงานในสังกัดสำนักบริหารการทะเบียน
- หน่วยงานระดับส่วนหรือเทียบเท่าในสังกัดสำนักบริหารการทะเบียน
- บริษัทที่เป็นผู้รับจ้างดำเนินงานโครงการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสารของสำนักบริหารการทะเบียน
- บริษัทหรือหน่วยงานที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน เห็นควรให้เข้าดำเนินการทดสอบระบบเพื่อเป็นประโยชน์ทางราชการ

(๒) หน่วยงานที่ขอเข้าปฏิบัติงานต้องทำหนังสือขออนุญาตถึงสำนักบริหารการทะเบียนเป็นผู้พิจารณาอนุญาต ได้แก่

- หน่วยงานราชการอื่นที่ไม่สังกัดสำนักบริหารการทะเบียน
- บริษัทที่เป็นผู้รับจ้างดำเนินงานโครงการของหน่วยงานราชการอื่นที่ไม่ได้สังกัดในสำนักบริหารการทะเบียน

(๓) ให้ระบุรายละเอียดการขอเข้าปฏิบัติงานในหนังสือขออนุญาตเข้าปฏิบัติงาน ดังนี้

- วัน – ช่วงเวลาในการเข้าปฏิบัติงาน
- รายชื่อเจ้าหน้าที่ประสานงาน
- รายชื่อเจ้าหน้าที่ที่จะเข้าปฏิบัติงาน
- วัตถุประสงค์การเข้าปฏิบัติงาน

(๔) หากมีการติดตั้งอุปกรณ์ให้แนบรายละเอียดอุปกรณ์ พร้อมรายละเอียดโครงการที่เกี่ยวข้องกับการติดตั้งอุปกรณ์

๑๔.๒ การใช้ห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ให้ปฏิบัติดังนี้

(๑) ให้ลงทะเบียนชื่อตามแบบฟอร์มทะเบียนผู้เข้าปฏิบัติงานห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ก่อนเข้าห้อง

(๒) ห้ามเข้าห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ก่อนได้รับอนุญาตจากผู้ดูแลเวรประจำวันหรือผู้ที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมอบหมาย

(๓) ห้ามเปิดประตูห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในห้องโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลเวรประจำวันหรือผู้ที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมอบหมาย และได้ลงทะเบียนชื่อตามแบบฟอร์มทะเบียนผู้เข้าปฏิบัติงานห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร เรียบร้อยแล้ว

(๔) ต้องแต่งกายให้สุภาพ

(๕) ห้ามสวมรองเท้าเข้าห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

(๖) ห้ามนำกระเป๋าเข้าห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

(๗) ห้ามสูบบุหรี่ หรือกระทำการอื่นใดที่อาจก่อให้เกิดฝุ่นละออง หรืออัคคีภัย

(๘) ห้ามนำอาหารหรือเครื่องดื่มเข้ามาในห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

(๙) ห้ามนำกล่องเครื่องมือหรือหีบห่อเข้าและออกห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ก่อนได้รับอนุญาตจากผู้ดูแลเวรประจำวันหรือผู้ที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมอบหมาย

(๑๐) ก่อนนำอุปกรณ์เข้าห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ต้องให้ผู้ดูแลเวรประจำวันหรือผู้ที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมอบหมายตรวจสอบก่อน

(๑๑) การนำอุปกรณ์เข้าติดตั้งชั่วคราวให้กรอกแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์ ก่อนและต้องได้รับอนุมัติก่อนจึงจะสามารถนำอุปกรณ์เข้าห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร และขอสำเนาแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์เพื่อใช้เป็นหลักฐานในกรณีนำอุปกรณ์ออก

(๑๒) การนำอุปกรณ์ออกต้องแสดงสำเนาแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์ที่เคยอนุมัติในข้อ ๑๔.๒ (๑๑) ให้ผู้ดูแลเวรประจำวันหรือผู้ที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมอบหมายตรวจสอบก่อน ในกรณีที่ไม่มีให้กรอกแบบฟอร์มการเคลื่อนย้าย วัสดุ/ครุภัณฑ์คอมพิวเตอร์ก่อนและต้องได้รับการอนุมัติ จึงจะสามารถนำอุปกรณ์ออกจากห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารได้

(๑๓) เมื่อปฏิบัติงานเสร็จแล้วให้กรอกแบบรายงนการเข้าปฏิบัติงานห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร แล้วให้ผู้ดูแลเวรประจำวันหรือผู้ที่ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนมอบหมายตรวจสอบก่อน

(๑๔) เวลาในการเข้าปฏิบัติงานห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

- ในเวลาราชการ ตอนเช้า เวลา ๐๘.๓๐ – ๑๒.๐๐ น.

ตอนบ่าย เวลา ๑๓.๐๐ – ๑๖.๓๐ น.

- นอกเวลาราชการให้มีคำสั่งหรือทำหนังสือขออนุญาต ตามขั้นตอนการขออนุญาตเข้าปฏิบัติงานห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ตามข้อ ๑๔.๑

๑๔.๓ ข้อกำหนดในการดูแลห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ให้ปฏิบัติดังนี้

(๑) บันทึกและจัดเก็บภาพของกล้องโทรทัศน์วงจรปิด (CCTV) ไว้อย่างน้อย ๑ เดือน เพื่อใช้ในการตรวจสอบภายหลัง

(๒) ตรวจสอบประตูเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารให้ปิดล็อกอยู่เสมอ

(๓) ต้องระมัดระวังดูแลสินทรัพย์สารสนเทศและให้มีการการบำรุงรักษาวัสดุอุปกรณ์ รวมทั้งระบบไฟฟ้า ระบบดับเพลิง ระบบปรับอากาศ หรือระบบอื่นใดที่ติดตั้งในห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารตามระยะเวลาที่เหมาะสม ให้มีสภาพพร้อมใช้งานอยู่เสมอ

(๔) ต้องดูแลความสะอาดและความเป็นระเบียบเรียบร้อยของห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารอย่างสม่ำเสมอ

๑๕. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator)

๑๕.๑ ผู้ดูแลระบบ แบ่งออกเป็น ๓ กลุ่ม ดังนี้

(๑) ผู้ดูแลระบบเครือข่าย (Network Administrator) มีหน้าที่และความรับผิดชอบดังนี้

- ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่ายและช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

- เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้นับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นระยะเวลาตามที่กฎหมายกำหนดนับตั้งแต่การใช้บริการสิ้นสุดลง และการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย

(๒) ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (Server Administrator) มีหน้าที่และความรับผิดชอบดังนี้

- ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานให้เป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าว

เกิดขึ้นจากการใช้งานของผู้ใช้ที่ไม่เป็นไปตามนโยบายนี้ให้รีบแจ้งผู้ใช้งานนั้นให้ยุติการกระทำในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้ทันที

- ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

- ติดตั้งโปรแกรมสำหรับจัดการซอฟต์แวร์ไม่ประสงค์ดีต่าง ๆ ให้เหมาะสม

- ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

- ดูแลรักษาและปรับปรุงระบบบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

(๓) ผู้ดูแลระบบสารสนเทศ (Application Administrator) มีหน้าที่และความรับผิดชอบดังนี้

- ดูแลรักษาและปรับปรุงบัญชีผู้ใช้ระบบสารสนเทศ ให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

- ปรับปรุงรายการระบบสารสนเทศและรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศนั้นให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

๑๕.๒ หลักธรรมาภิบาลของผู้ดูแลระบบ มีดังนี้

(๑) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้โดยไม่มีเหตุผลอันสมควร

(๒) ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

(๓) ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๑๖. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log Management)

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ให้ปฏิบัติดังนี้

๑๖.๑ ต้องกำหนดผู้รักษาข้อมูลจราจรคอมพิวเตอร์ประจำหน่วยงาน และมี Log Server ของหน่วยงาน สำหรับรวบรวมข้อมูลจราจรคอมพิวเตอร์ที่พร้อมส่งมอบให้ผู้รักษาข้อมูลจราจรคอมพิวเตอร์ของหน่วยงานเมื่อมีการร้องขอ

๑๖.๒ กำหนดวิธีการในการนำส่งข้อมูลจราจรคอมพิวเตอร์จากสื่อที่ใช้เก็บไปยัง Centralized Log Server ของหน่วยงาน

๑๖.๓ บันทึกการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุกได้แก่ บันทึกการเข้า-ออกระบบ ซึ่งประกอบด้วย บัญชีผู้ใช้ (Account) หมายเลขไอพีแอดเดรส (IP Address) ต้นทาง หมายเลขไอพีแอดเดรส (IP Address) ปลายทาง โปรโตคอล (Protocol) และหมายเลขพอร์ต (Port Number) เพื่อประโยชน์ในการใช้ตรวจสอบและเก็บบันทึกดังกล่าวไว้ตามกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๑๖.๔ ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๑๖.๕ กำหนดวิธีการป้องกันการแก้ไข เปลี่ยนแปลง หรือทำลาย ข้อมูลจราจรคอมพิวเตอร์ต่าง ๆ และจำกัดสิทธิการเข้าถึงข้อมูลจราจรคอมพิวเตอร์เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ ๒

นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถใช้งานได้อย่างต่อเนื่อง

๒. เพื่อเป็นมาตรฐานแนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงาน เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. การคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๑.๑ ต้องจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑.๒ ชนิดข้อมูลที่ต้องสำรองอย่างน้อยต้องประกอบด้วย

(๑) ค่า Configuration สำหรับระบบ

(๒) ข้อมูลคู่มือการปฏิบัติงานสำหรับระบบ

(๓) ฐานข้อมูลของระบบสารสนเทศของหน่วยงาน

(๔) ซอฟต์แวร์ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ระบบงาน หรือซอฟต์แวร์อื่นใดที่เห็นควรทำการสำรอง

๑.๓ กำหนดขั้นตอนและความถี่ในการสำรองและกู้คืนข้อมูลอย่างถูกต้องและชัดเจน

๑.๔ กำหนดรูปแบบการสำรองข้อมูล การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup) ให้เหมาะสมกับข้อมูลที่จะทำการสำรอง

๑.๕ ต้องบันทึกข้อมูล ผู้ดำเนินการ วันที่ เวลา ชื่อข้อมูลที่สำรอง สถานะการสำรองข้อมูล

๑.๖ จัดเก็บข้อมูลที่สำรองนั้นในสื่อบันทึกข้อมูล โดยพิมพ์ชื่อบนสื่อบันทึกข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

๑.๗ จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ และดำเนินการป้องกันทางกายภายอย่างเพียงพอต่อสถานที่สำรอง ที่ใช้จัดเก็บข้อมูล

๑.๘ กำหนดให้มีการใช้งานการเข้ารหัส (Encryption) กับข้อมูลลับที่ได้สำรองเก็บไว้

๒. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

๒.๑ กำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๒ ต้องประเมินสถานการณ์ความเสี่ยงสำหรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ

๒.๓ กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๒.๔ กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอกที่จะต้องติดต่อเมื่อเกิดเหตุจำเป็นฉุกเฉิน

๒.๕ สร้างความตระหนัก ให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ สิ่งที่ต้องดำเนินการเมื่อเกิดเหตุเร่งด่วน หรือความรู้อื่นใดในการเตรียมความพร้อมกรณีฉุกเฉิน

๒.๖ ต้องทดสอบสภาพความพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓

นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. ผู้ตรวจสอบ (Audit)

แนวปฏิบัติ

๑. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

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

๑.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๑.๓ มีการตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบ (Audit) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

๒. การดำเนินการตรวจสอบและประเมินความเสี่ยง

๒.๑ ผู้ตรวจสอบ (Audit) สามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านอย่างเดียว

๒.๒ ในกรณีจำเป็นต้องเข้าถึงข้อมูลแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบ (Audit) ใช้งาน รวมทั้งให้มีการทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๒.๓ มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๒.๔ มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ (Audit) รวมทั้งบันทึกประวัติแสดงการเข้าถึง (Logs) นั้น ซึ่งรวมถึงวันที่และเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

๒.๕ ในกรณีที่มีเครื่องมือสำหรับตรวจประเมินระบบสารสนเทศ แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

๓. การบริหารความต่อเนื่องของระบบสารสนเทศ

๓.๑ มีระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) สอดคล้องกับการใช้งานตามภารกิจของหน่วยงาน

๓.๒ มีการปรับปรุงระบบสารสนเทศ ระบบสำรอง และแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) อย่างน้อยปีละ ๑ ครั้ง ทั้งนี้ให้ความถี่เพียงพอสภาพความเสี่ยงที่ยอมรับได้

๓.๓ มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) อย่างน้อยปีละ ๑ ครั้ง ทั้งนี้ให้ความถี่เพียงพอสภาพความเสี่ยงที่ยอมรับได้

๓.๔ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๓.๕ ในการสำรองข้อมูลให้มีการคัดเลือกและจัดทำระบบสำรองที่เหมาะสม

๓.๖ จัดทำคู่มือที่เกี่ยวข้องกับการปฏิบัติงานตามแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๔. การแจ้งเหตุด้านความมั่นคงปลอดภัย

๔.๑ แจ้งไปยังผู้ดูแลระบบของส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียนโดยทันที เมื่อพบเหตุ

(๑) การกระทำผิดที่ขัดต่อกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

(๒) การกระทำผิดที่ขัดต่อความมั่นคงของชาติ

(๓) การใช้ทรัพยากรสารสนเทศของหน่วยงานไม่เหมาะสม ผิดวัตถุประสงค์

(๔) หน้าเว็บไซต์หลัก หรือระบบงานของหน่วยงานถูกเปลี่ยนแปลงโดยผู้ไม่ประสงค์ดี

(๕) ข้อมูลเว็บไซต์หลัก หรือระบบงานของหน่วยงานไม่ถูกต้อง หรือคลาดเคลื่อนจากความเป็นจริง

(๖) ข้อมูลสารสนเทศสำคัญของหน่วยงานหรือส่วนตัวถูกเปิดเผย เปลี่ยนแปลง ลบ หรือสูญหายโดยไม่ได้รับอนุญาต

(๗) มีการนำข้อมูลสารสนเทศสำคัญของหน่วยงานไปใช้ผิดวัตถุประสงค์

(๘) ทรัพยากรสารสนเทศถูกขโมย หรือสูญหาย

(๙) มีบุคลาการภายนอกเข้าใช้งานระบบสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาต

(๑๐) มีการแอบติดตั้งอุปกรณ์ หรือโปรแกรมเพื่อดักขโมยข้อมูล หรือดักฟัง ดักดูข้อมูลในระบบเครือข่ายของหน่วยงาน

(๑๑) มีการใช้อำนาจของสิทธิการเป็นผู้ดูแลระบบอย่างไม่เหมาะสม

(๑๒) มีการบุกรุกห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารของหน่วยงาน

(๑๓) มีการบุกรุกหรือการใช้โปรแกรมของผู้ไม่ประสงค์ดี

(๑๔) เหตุการณ์อื่น ๆ ที่เป็นการละเมิดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๔.๒ การจัดการกับเหตุด้านความมั่นคงปลอดภัยด้านสารสนเทศ เมื่อได้รับรายงานเหตุด้านความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้ดูแลระบบที่ได้รับมอบหมายปฏิบัติตามแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๔.๓ ให้ความร่วมมือและให้ความสะดวกแก่ผู้บังคับบัญชา ผู้ดูแลระบบที่เกี่ยวข้องในการตรวจเหตุการณ์ทางด้านความมั่นคงปลอดภัยด้านสารสนเทศที่เกิดขึ้น รวมทั้งปฏิบัติตามคำแนะนำของผู้บังคับบัญชาและผู้ดูแลระบบที่เกี่ยวข้อง

ส่วนที่ ๔

นโยบายสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศให้กับผู้ใช้งานของหน่วยงาน

๒. เพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการ

๓. เพื่อให้การใช้งานระบบสารสนเทศมีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

การฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน

๑.๑ จัดฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๑.๒ จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของหน่วยงาน

๑.๓ จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

๑.๔ จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดให้ความรู้

๑.๕ ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

๑.๖ ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)
สำนักบริหารการทะเบียน

๑. หลักการและเหตุผล

ข้อมูลสารสนเทศซึ่งจัดเก็บไว้ที่ห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ถือเป็นสินทรัพย์ทางการบริหารที่สำคัญของสำนักบริหารการทะเบียน จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการวางแผนด้านการบริหารและการให้บริการ ดังนั้น เพื่อป้องกันปัจจัยจากภายนอกและปัจจัยภายในมากระทบ และทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งอุปกรณ์ต่าง ๆ เกิดความเสียหายได้ สำนักบริหารการทะเบียนจึงได้จัดทำแผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ ป้องกันและแก้ไขปัญหาที่อาจกระทบต่อระบบเทคโนโลยีสารสนเทศของสำนักบริหารการทะเบียน

๒. วัตถุประสงค์

๒.๑ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติงาน ในการดูแลระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๒.๒ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสำนักบริหารการทะเบียน ให้มีเสถียรภาพและมีความพร้อมใช้งาน

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินและลดความเสียหายที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของสำนักบริหารการทะเบียน

๓. เหตุภัยพิบัติ

ภัยพิบัติเป็นภัยที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของสำนักบริหารการทะเบียน ซึ่งสามารถจำแนกประเภทได้ ดังนี้

๓.๑ ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ได้แก่ อัคคีภัย อุทกภัย เป็นต้น

๓.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓.๓ ระบบสื่อสารของห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารที่เชื่อมต่อกับระบบเครือข่ายภายนอกขัดข้อง

๓.๔ กระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๓.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายข้อมูล

๓.๖ ไวรัสคอมพิวเตอร์

๓.๗ ระบบเสียหายจากภัยสงคราม เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

๓.๘ ระบบเทคโนโลยีสารสนเทศหลักเสียหาย หรือข้อมูลถูกทำลาย

๓.๙ การบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตีระบบเครือข่าย

๓.๑๐ ผลกระทบจากความชื้นและอุณหภูมิที่ไม่เหมาะสม

๔. แนวทางการป้องกันและแก้ไขความเสียหายจากภัยพิบัติ

๔.๑ ภัยธรรมชาติ

ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร ได้แก่ อัคคีภัย อุทกภัย เป็นต้น

(๑) การป้องกันอัคคีภัย

- กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนให้มองเห็นชัดเจน
- จัดอบรมแผนป้องกันและระงับอัคคีภัย ซ้อมดับเพลิงและการหนีไฟขั้นต้นให้แก่บุคลากรในหน่วยงานทุกคน อย่างน้อยปีละ ๑ ครั้ง
- จัดทำระบบดับเพลิงอัตโนมัติสำหรับห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

(๒) การป้องกันอุทกภัย

- ตรวจสอบการรั่วซึมของหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำฝนที่ค้างสะสม

๔.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

(๑) ควบคุมการเข้า-ออกห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้อง หากจำเป็นให้มีเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้รับผิดชอบนำเข้าไป

(๒) จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบยืนยันตัวตนด้วยลายนิ้วมือ (Finger Scan)

(๓) มีเวรเฝ้าระวังและตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

(๔) ติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

๔.๓ ระบบสื่อสารของห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารที่เชื่อมต่อกับระบบเครือข่ายภายนอกขัดข้อง

(๑) ตรวจสอบและเฝ้าระวังระบบเครือข่ายทั้งภายในและภายนอกให้สามารถใช้งานได้ตลอดเวลา

(๒) ต้องจัดให้มีเครือข่ายสำรอง กำหนดให้ใช้งานได้ในกรณีที่ระบบสื่อสารเส้นทางหลักไม่สามารถใช้งานได้

๔.๔ กระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

(๑) มีระบบสำรองไฟฟ้าและปรับแรงดันอัตโนมัติเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๓๐ นาที

(๒) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาให้บริการ ตรวจสอบการทำงานของระบบทุกวัน และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอย่างน้อยเดือนละ ๑ ครั้ง

๔.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายข้อมูล

(๑) ติดตั้งระบบป้องกันการบุกรุกเครือข่าย เพื่อตรวจสอบและป้องกันผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ต (Internet) และอินทราเน็ต (Intranet) สามารถเข้าสู่ระบบตลอดเวลา

(๒) จัดเวรเฝ้าระวังระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ต (Internet) และอินทราเน็ต (Intranet) เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือมีความถี่ในการเรียกใช้งานผิดปกติเพื่อจะได้สรุปหาสาเหตุและป้องกัน

(๓) ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และปรับปรุงอย่างสม่ำเสมอ และปิดพอร์ต (Port) ที่ไม่มีการใช้งาน

(๔) กำหนดรหัสผ่าน (Password) เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

(๕) ป้องกันการปลอมแปลงหมายเลขไอพีแอดเดรส (IP Address) โดยการกรองแพ็คเกท (Package) ที่มาจากภายนอก

๔.๖ ไวรัสคอมพิวเตอร์

(๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดท (Update) ข้อมูลไวรัสอยู่เสมอ และต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

(๒) ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่าง ๆ

(๓) ใช้ความระมัดระวังในการเปิดจดหมายอิเล็กทรอนิกส์ (E-Mail)

(๔) ระมัดระวังการดาวน์โหลดไฟล์ต่าง ๆ จากอินเทอร์เน็ต (Internet)

๔.๗ ระบบเสียหายจากภัยสงคราม เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

เนื่องจากภัยดังกล่าวเป็นภัยจากปัจจัยภายนอกที่ไม่สามารถยับยั้งได้ สามารถป้องกันได้โดยการจัดทำระบบคอมพิวเตอร์กลางและระบบสื่อสารสำรอง และมีระบบสำรองข้อมูลโดยแยกสถานที่จัดเก็บมากกว่า ๑ แห่ง หากเกิดความเสียหายกับข้อมูล สามารถนำข้อมูลที่มีในระบบคอมพิวเตอร์กลางและระบบสื่อสารสำรองหรือข้อมูลในระบบสำรองที่จัดเก็บไว้มาใช้แทนได้ทันที

๔.๘ ระบบเทคโนโลยีสารสนเทศหลักเสียหาย หรือข้อมูลถูกทำลาย

(๑) กำหนดให้มีการสำรองข้อมูลอัตโนมัติไปยังฮาร์ดดิสก์ภายนอก (External Hard Disk) และเครื่องคอมพิวเตอร์แม่ข่ายที่ไซต์สำรอง (Disaster Recovery Site: DR Site) ซึ่งเครื่องจะบันทึกประวัติการทำงานไว้

(๒) ทดสอบกู้คืนข้อมูลและฐานข้อมูล ที่ได้สำรองไว้อย่างสม่ำเสมอทุกระบบอย่างน้อยปีละ ๑ ครั้ง

(๓) บำรุงรักษาข้อมูลและระบบสำรอง เพื่อลดความเสียหายของข้อมูล

๔.๙ การบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

(๑) มีระบบยืนยันตัวตน (Identification) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ต (Internet) และอินทราเน็ต (Intranet) หรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

(๒) กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

(๓) หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าไปในห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร จะต้องให้เจ้าหน้าที่ผู้ดูแลห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารเป็นผู้รับผิดชอบนำเข้าไป และคอยกำกับดูแลตลอดการปฏิบัติงาน สำหรับประตูเข้า-ออกมีการติดตั้งระบบสแกนลายนิ้วมือ (Finger Scan) และติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) เพื่อป้องกันการโจรกรรม

(๔) ติดตั้งระบบป้องกันการบุกรุกเครือข่าย เพื่อตรวจสอบและป้องกันผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ต (Internet) และอินทราเน็ต (Intranet) สามารถเข้าสู่ระบบตลอดเวลา

(๕) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ต (Internet) และอินทราเน็ต (Intranet) เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือมีความถี่ในการเรียกใช้งานผิดปกติเพื่อจะได้สรุปหาสาเหตุและป้องกัน

๔.๑๐ การป้องกัน ความชื้นและอุณหภูมิที่ไม่เหมาะสม

เปิดเครื่องปรับอากาศและเครื่องควบคุมความชื้น และติดตั้งระบบอัตโนมัติตรวจสอบการทำงานตลอด ๒๔ ชั่วโมง

๕. การกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติ

การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย ต้องอยู่ในสภาพพร้อมให้บริการได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเกิดความเสียหายหรือหยุดทำงาน ต้องดำเนินการ ดังนี้

๕.๑ ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

๕.๒ จัดหาอุปกรณ์หรือชิ้นส่วนเพื่อทดแทน

๕.๓ ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน ๔๘ ชั่วโมง

๕.๔ นำข้อมูลจากสื่อบันทึกข้อมูลสำรองหรือจากระบบสำรองข้อมูลกลับมาใช้งานโดยเร็วภายใน ๔๘ ชั่วโมง

๖. ผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

หน่วยงานต้องจัดเตรียมผู้รับผิดชอบและมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

๖.๑ ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติการ ผู้รับผิดชอบ ได้แก่

(๑) ผู้บริหารระดับสูงสุดของหน่วยงาน

(๒) ผู้เชี่ยวชาญเฉพาะด้านเทคโนโลยีสารสนเทศและระบบข้อมูล

(๓) ผู้เชี่ยวชาญเฉพาะด้านการบริหารงานทะเบียน

(๔) ผู้อำนวยการส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน

๖.๒ ระดับปฏิบัติการ

(๑) ผู้ดูแลระบบเครือข่าย (Network Administrator) โดย กลุ่มงานควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารงานทะเบียน ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน ทำหน้าที่

- กู้คืนระบบเครือข่ายและสื่อสารให้ทำงานได้ปกติ
- หาสาเหตุและอุดช่องโหว่ระบบเครือข่าย เพื่อป้องกันภัยคุกคามทางคอมพิวเตอร์
- จัดเตรียมสถานที่สำหรับไซต์สำรอง (Disaster Recovery Site: DR Site) รวมถึงระบบไฟฟ้า ระบบสื่อสาร ระบบปรับอากาศให้พร้อมใช้งาน

(๒) ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (Server Administrator) โดย กลุ่มงานควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารงานทะเบียน ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน ทำหน้าที่

- กู้คืนเมื่อเครื่องคอมพิวเตอร์แม่ข่ายไม่ทำงาน
- เฝ้าระวังการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบเทคโนโลยีสารสนเทศของหน่วยงาน
- ดูแลการสำรองและกู้คืนข้อมูลและฐานข้อมูลจากความเสียหายให้กลับมาใช้งานตามปกติ

(๓) ผู้ดูแลระบบไฟฟ้า (Electrical Administration) ประกอบด้วย กลุ่มงานควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารงานทะเบียน ส่วนบริหารและพัฒนาเทคโนโลยีการทะเบียน และกลุ่มงานบริหารทั่วไป ทำหน้าที่

- ติดตั้งระบบดับเพลิงอัตโนมัติในห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสาร

- ดูแลและบำรุงรักษาอุปกรณ์ในห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารไซต์สำรอง (Disaster Recovery Site: DR Site)

- ดูแลและบำรุงรักษาระบบไฟฟ้า ระบบปรับอากาศ การควบคุมความชื้นห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารและห้องควบคุมระบบคอมพิวเตอร์กลางและระบบสื่อสารไซต์สำรอง (Disaster Recovery Site: DR Site)

- ดูแลระบบแจ้งเตือนระบบไฟฟ้าขัดข้องนอกเวลาราชการ เพื่อให้เจ้าหน้าที่ผู้รับผิดชอบสามารถเข้าไปแก้ไขปัญหาได้อย่างรวดเร็ว

- ตรวจสอบและเตรียมน้ำมันสำรองสำหรับเครื่องกำเนิดไฟฟ้า เพื่อให้เครื่องพร้อมใช้งานเมื่อเกิดเหตุไฟฟ้าขัดข้องหรือไฟฟ้าดับ

- รับผิดชอบการเปิดเครื่องกำเนิดไฟฟ้าเมื่อเกิดเหตุไฟฟ้าขัดข้องหรือไฟฟ้าดับ

- จัดเวรเฝ้าระวังระบบไฟฟ้า

๗. การทบทวนและปรับปรุงแผน

แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ต้องได้รับการปรับปรุงให้สามารถปรับใช้ได้อย่างเหมาะสม และสอดคล้องกับการใช้งานตามภารกิจตามที่ระบุ อย่างน้อยปีละ ๑ ครั้ง

๘. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้บริหารทราบตามลำดับชั้นเป็นประจำทุกเดือน เพื่อรายงานสรุปให้ผู้บริหารระดับสูงสุดของหน่วยงานทราบ และหากมีเหตุฉุกเฉินร้ายแรงต้องรายงานให้ผู้บริหารระดับสูงสุดของหน่วยงานทราบทันที