ประกาศสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน)
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำประกาศแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

ดังนั้น เพื่อให้การปฏิบัติงานและการบริหารงานมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล สำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) (สพพ.) จึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) เพื่อเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒”

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓. สำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) ได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) เป็นลายลักษณ์อักษรตามเอกสารแนบท้ายประกาศ ประกอบด้วยเนื้อหาอย่างน้อยครอบคลุมตามประกาศนี้มี ๒ ส่วน ดังนี้

๓.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาตามที่กำหนดในข้อ ๔

๓.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาตามที่กำหนดในข้อ ๕ - ๑๕

ข้อ ๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มีดังนี้

๔.๑ การจัดทำนโยบายต้องมีผู้บริหาร เจ้าหน้าที่ปฏิบัติงานด้านคอมพิวเตอร์ และผู้ใช้งานมีส่วนร่วมในการจัดทำนโยบาย

๔.๒ นโยบายต้องจัดทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน)

๔.๓ มีการกำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวไว้ชัดเจน

๔.๔ มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๔.๕ มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ การควบคุมการเข้าถึงสารสนเทศและการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๔.๖ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ ไม่พึงเปิดเผย

๔.๗ มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

๔.๘ มีนโยบายในการบริหารจัดการระบบเทคโนโลยีสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภท และจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๔.๙ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๔.๑๐ มีนโยบายให้มีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔.๑๑ การสร้างความรู้ความเข้าใจในการใช้ระบบเทคโนโลยีสารสนเทศและระบบคอมพิวเตอร์

๔.๑๒ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งาน ทั้งภายในและภายนอก

ข้อ ๕. การเข้าถึงหรือควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ (Access Control) ประกอบด้วย

๕.๑ มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยเป็นสำคัญ

๕.๒ ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

๕.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้น ความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ซึ่งได้รับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ประกอบด้วย

๖.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัย และผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๖.๒ การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งาน เมื่อมีการอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๖.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิ เพื่อเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

๖.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๖.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบเทคโนโลยีสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๗. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ประกอบด้วย

๗.๑ การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งาน ในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๗.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๗.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศ เมื่อว่างเว้นจากการใช้งาน

๗.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๘. การบริหารจัดการการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ประกอบด้วย

๘.๑ ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ ได้แก่ โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๘.๒ ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๘.๓ ผู้ดูแลระบบ ควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๘.๔ ผู้ดูแลระบบ ควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced path) จากเครื่องลูกข่าย ไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

๘.๕ การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๘.๖ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการภายใต้การควบคุมของเจ้าหน้าที่สารสนเทศเท่านั้น

๘.๗ ใช้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อควบคุมและติดตามผู้ใช้งานระบบ

๘.๘ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้วิธีการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง

๘.๙ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ผู้ใช้ระบบทุกคน เมื่อจะเข้าใช้งานระบบของสำนักงาน

๘.๑๐ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) เพื่อควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพ และทางเครือข่าย

๘.๑๑ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) เพื่อควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน หรือเชื่อมต่อระหว่างหน่วยงาน

๘.๑๒ มีการควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์ และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ

ข้อ ๙. การบริหารจัดการการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ประกอบด้วย

๙.๑ การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๙.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

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

๙.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๙.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out)

๙.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบเทคโนโลยีสารสนเทศ หรือโปรแกรมที่มีความเสี่ยง หรือมีความสำคัญสูง

ข้อ ๑๐. การบริหารจัดการการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (Application and Information Access Control) ประกอบด้วย

๑๐.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) หรือควบคุมการเข้าถึง การใช้งานของผู้ใช้งานงานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๑๐.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking)

๑๐.๓ การควบคุมคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ได้ กำหนดข้อปฏิบัติและมาตรการที่ เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารตามความเหมาะสม

๑๐.๔ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) ต้องกำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ข้อ ๑๑. การจัดทำระบบสำรองสำหรับระบบเทคโนโลยีสารสนเทศ ประกอบด้วย

๑๑.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๑๑.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๑๑.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๑.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ

๑๑.๕ สำหรับความถี่ของการปฏิบัติในแต่ละข้อ ควรมีการปฏิบัติที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน

ข้อ ๑๒. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ประกอบด้วย

๑๒.๑ หน่วยงานของรัฐต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๑๒.๒ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ข้อ ๑๓ สำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) กำหนดความรับผิดชอบให้เป็นไปตามเอกสารแนบท้ายประกาศ ส่วนที่ ๑๒

๑๓.๑ ระดับนโยบาย

กำหนดให้ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นในกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศ เกิดความเสียหายหรืออันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืน การปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

กำหนดให้ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (Chief Information Officer : CIO) เป็นผู้รับผิดชอบติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะ ให้คำปรึกษาแก่เจ้าหน้าที่

ข้อ ๑๔ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยอ้างอิงรายละเอียดแนวปฏิบัติเอกสารแนบท้าย “แนวนโยบายและแนวปฏิบัติในการักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) พ.ศ. ๒๕๖๒” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ของหน่วยงานและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

ประกาศ ณ วันที่ ๔ มิถุนายน พ.ศ. ๒๕๖๒

(นายพีรเมศร์ วุฒิธรเนติรักษ์)
ผู้อำนวยการ สพพ.

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

พ.ศ. ๒๕๖๓

สำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน)

คำนำ

ตามที่ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการกิจกรรมหรือการให้บริการต่างๆ ของหน่วยงานรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

ดังนั้น สำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) (สพพ.) จึงได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) พ.ศ. ๒๕๖๒ เพื่อให้การดำเนินด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๒ จากบุคลากรทุกคน และต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว สพพ. จึงหวังเป็นอย่างยิ่งว่าแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้ จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของ สพพ. ทุกคน ถือปฏิบัติโดยเคร่งครัดต่อไป

คณะทำงานจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สพพ.

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) พ.ศ. ๒๕๖๒

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) หรือต่อไปนี้เรียกว่า สพพ. เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่องค์กร และหน่วยงานในสังกัด สพพ. จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ โดยมีขอบเขต และวัตถุประสงค์ ดังต่อไปนี้

๑. ขอบเขตการดำเนินการ

๑) การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพพ. มีขอบเขตครอบคลุมการบริหารจัดการ การรักษาความมั่นคงปลอดภัยทางกายภาพ การควบคุมการเข้าถึงข้อมูล และระบบสารสนเทศ การใช้งานเครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์พกพา รวมถึงอุปกรณ์ต่างๆ และการใช้งานระบบเครือข่ายสื่อสารข้อมูล ภายใน สพพ. เครือข่ายอินเตอร์เน็ต และจดหมายอิเล็กทรอนิกส์

๒) การบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพพ. อ้างอิงตามมาตรฐาน ISO/IEC ๒๗๐๐๑

๓) นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับใน สพพ. ได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๔) นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินผลการปฏิบัติเพื่อปรับนโยบายตามระยะเวลา ๑ ครั้ง ต่อปี

๒. วัตถุประสงค์

๑) เพื่อให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒) เพื่อกำหนดแนวทางและวิธีการปฏิบัติสำหรับบุคลากรและบุคคลที่ปฏิบัติงานสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) ในการยืนยันตัวบุคคลการเข้าถึง และการควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ

๓) เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีแผนเตรียมความพร้อมกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ตามปกติ ให้มีระบบสำรองสามารถทำงานได้อย่างต่อเนื่องและสามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม

๔) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๕) เพื่อสร้างความตระหนักและส่งเสริมให้เกิดความรู้ ความเข้าใจ และการให้การอบรมทางด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศให้แก่บุคลากรและบุคคลที่เกี่ยวข้อง

องค์ประกอบของนโยบาย

๑. คำนิยาม
๒. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
๓. การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย และศูนย์ข้อมูล
๔. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
๕. การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
๖. การใช้งานอินเทอร์เน็ต
๗. การใช้งานจดหมายอิเล็กทรอนิกส์
๘. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
๙. ระบบปลอดภัยความปลอดภัย
๑๐. แผนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และภัยพิบัติที่อาจเกิดขึ้นกับระบบ Server และเครือข่าย สพพ.

องค์ประกอบของนโยบายการการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพพ. แต่ละส่วนที่กล่าวข้างต้น จะประกอบด้วย วัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของ สพพ. เพื่อที่จะทำให้ สพพ. มีมาตรการในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากรของ สพพ. ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพพ. นี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพพ. ซึ่งเจ้าหน้าที่ของ สพพ. และหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

สพพ. หมายความว่า สำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน)

ผู้บังคับบัญชา หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ สพพ.

ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) หมายความว่า ผู้อำนวยการสำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) หมายความว่า ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารของ สพพ.

ฝ่ายสารสนเทศ หมายความว่า หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ ระบบชุดคำสั่ง ชุดคำสั่ง โปรแกรม และเครือข่ายใน สพพ.

เทคโนโลยีสารสนเทศ (Information Technology) หมายความว่า เทคโนโลยีสำหรับการประมวลผลสารสนเทศ ซึ่งจะครอบคลุมถึงการรับส่ง แปลง ประมวลผล และสืบค้นสารสนเทศ โดยมีองค์ประกอบ ๓ ส่วน คือ คอมพิวเตอร์ การสื่อสารและสารสนเทศ ซึ่งต้องอาศัยการทำงานร่วมกัน

ความลับ (Confidentiality) หมายความว่า การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับ และจะมีเพียงผู้มีสิทธิ์เท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

ความมั่นคง (Integrity) หมายความว่า การรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิ์ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

ความพร้อมใช้งาน (Availability) หมายความว่า การรับรองได้ว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

การพิสูจน์สิทธิ์ (Authentication) หมายความว่า การตรวจสอบสิทธิ์ และลำดับชั้นของสิทธิ์ในการขอเข้าใช้ระบบของผู้ใช้บริการ จากรายชื่อผู้มีสิทธิ์สำหรับอุปกรณ์ไอที รวมถึงแอพพลิเคชันทั้งหลาย

การรับรองสิทธิ์ (Authorization) หมายความว่า การตรวจสอบว่า บุคคล อุปกรณ์ไอที หรือแอพพลิเคชันนั้นๆ ได้รับอนุญาตให้ดำเนินการอย่างหนึ่งอย่างใดต่อระบบสารสนเทศหรือไม่

การเก็บสำรองข้อมูล (Data backup) หมายความว่า การเก็บสำรอง สำเนาของชุดข้อมูลปัจจุบัน ที่ถูกสร้างขึ้นมา เพื่อป้องกันการสูญหายของข้อมูล

การปกป้องข้อมูล (Data protection) หมายความว่า การป้องกันการเข้าถึงข้อมูลตามลำดับชั้นความลับ และข้อมูลส่วนบุคคล ต่อบุคคลที่ไม่มีส่วนเกี่ยวข้อง

การรักษาความมั่นคงปลอดภัย หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพพ.

การรักษาความปลอดภัยของข้อมูล (Data security) หมายความว่า การป้องกันข้อมูลในบริบทของการรักษาความลับ ความมั่นคง และความพร้อมใช้งานของข้อมูล

การประเมินความเสี่ยง หรือการวิเคราะห์ความเสี่ยง (Risk assessment or analysis) ของระบบสารสนเทศ หมายความว่า การตรวจสอบปัจจัยและโอกาสของเหตุการณ์ใดๆ ที่ไม่พึงประสงค์ ต่อระบบฯ และ ผลเสียที่อาจจะเกิดขึ้นตามมาได้

“นโยบายด้านความมั่นคงปลอดภัย (Security policy)” หมายความว่า นโยบายที่แสดงเป้าหมายที่จะต้องปกป้อง และขั้นตอนทั่วไปของกระบวนการรักษาความมั่นคงปลอดภัย ในบริบทของความต้องการอย่างเป็นทางการขององค์กร

มาตรฐาน (Standard) หมายความว่า บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

วิธีการปฏิบัติ (Procedure) หมายความว่า รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวทางปฏิบัติ (Guideline) หมายความว่า แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้ หมายความว่า บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหารหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของ สพพ. โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (role) ซึ่งองค์กรกำหนดไว้ ดังนี้

ผู้บริหาร หมายความว่า ผู้มีอำนาจบริหารในระดับสูงของ สพพ.

ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ และบุคลากรภายนอก

ผู้ดูแลระบบ (System Administrator) หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

เจ้าหน้าที่ หมายความว่า ผู้บริหาร เจ้าหน้าที่ พนักงาน และลูกจ้างขององค์กร

หน่วยงานภายนอก หมายความว่า องค์กรหรือหน่วยงานที่ สพพ. อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูล หรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

สารสนเทศ (Information) หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนาไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของ สพพ. ได้ ได้แก่ ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเตอร์เน็ต (Internet)

ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเตอร์เน็ต (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายความว่า ระบบงานของหน่วยงาน ที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศ ที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspace) หมายความว่า พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

- พื้นที่ทำงานทั่วไป (General Working Area) หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล
- พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)
- พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area)
- พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

เจ้าของข้อมูล หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้น เกิดสูญหาย

สิทธิ์ผู้ใช้งาน หมายความว่า สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์ใดที่ เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน โดยหน่วยงานจะเป็นผู้พิจารณาสิทธิ์ในการใช้ทรัพย์สิน

สินทรัพย์ หมายความว่า ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของ สพพ. ได้แก่ เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

จดหมายอิเล็กทรอนิกส์ (E-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

บัญชีผู้ใช้งาน (Account) หมายความว่า รายชื่อผู้มีสิทธิ์ใช้งานเครื่องคอมพิวเตอร์ และบริการในระบบ เครือข่ายของ สพพ.

ข้อมูลจราจรทางคอมพิวเตอร์ (Log) หมายถึง ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิด ของบริการอื่นๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

ชุดคำสั่งไม่พึงประสงค์ หมายความว่า ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์หรือชุดคำสั่งอื่น เกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การตรวจสอบการอนุมัติ และการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานในการผ่านเข้าถึงระบบเครือข่ายหรือระบบเทคโนโลยีสารสนเทศให้แก่ผู้ใช้ที่เจ้าของข้อมูลอนุญาตให้ใช้งานระบบเทคโนโลยีสารสนเทศนั้นๆ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายความว่า การธำรงไว้ ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

สถานการณ์ความเสี่ยง หมายความว่า เหตุการณ์ที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศของ สพพ.สามารถแยกเป็นภัยต่างๆ ได้ ๔ ประเภท ได้แก่ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error), ภัยที่เกิด Software, ภัยจากไฟไหม้ หรือระบบไฟฟ้า และภัยจากน้ำท่วม (อุทกภัย)

สถานการณ์ความไม่แน่นอนและภัยพิบัติ หมายความว่า บุคลากรของหน่วยงาน สถานการณ์หรือเหตุการณ์ ทั้งเจตนาและไม่เจตนา อันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผยหรือเปลี่ยนแปลง ทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่นๆ

แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติ หมายความว่า ข้อปฏิบัติในการแก้ไขปัญหาเมื่อเกิดสถานการณ์ความไม่แน่นอน หรือภัยพิบัติ แบ่งเป็น ๓ ด้าน ได้แก่ แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์ (Contingency Plan) แผนดำเนินการเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan) และแผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Procedure)

ส่วนที่ ๑
การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and environment security)

๑. วัตถุประสงค์

กำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับ การเข้าใช้งานหรือการเข้าถึงอาคารสถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตาม ความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศ และข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่า และอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้ จะมีผลบังคับใช้กับผู้ใช้งาน ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพพ.

๒. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๑) ภายใน สพพ. มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสมโดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General working area) พื้นที่ทำงานของผู้ดูแลระบบ (System administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN coverage area) เป็นต้น

๓) ผู้ดูแลระบบ ต้องกำหนดสิทธิ์ให้กับเจ้าหน้าที่ ให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

(๓.๑) จัดทำ “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(๓.๒) ทำการบันทึกการเข้าออกพื้นที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้าออกพื้นที่”

(๓.๓) จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกเดือน และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างน้อยปีละ ๑ ครั้ง

การควบคุมการเข้าออก อาคารสถานที่

๑) จัดทำเอกสารระบุสิทธิ์ของ ผู้ใช้งาน และ “หน่วยงานภายนอก” ในการเข้าถึงสถานที่ ประกอบด้วย

(๑.๑) กำหนดสิทธิ์ผู้ใช้งาน ที่มีสิทธิ์ผ่านเข้าออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออก ในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

(๑.๒) การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ ได้แก่ บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึก และรับแบบฟอร์มการเข้าออก หรือ บัตรผู้ติดต่อ (Visitor)

(๑.๓) บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ในตำแหน่งที่สามารถเห็นได้ชัดเจน ตลอดเวลา ที่อยู่ใน สพพ.

(๑.๔) เจ้าหน้าที่ที่บุคคลภายนอกเข้ามาติดต่อ จะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกให้ถูกต้อง หรือ จัดให้มีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

(๑.๕) บุคคลภายนอกหรือผู้ติดต่อ ต้องคืนแบบฟอร์มการเข้าออก หรือ บัตรผู้ติดต่อ (Visitor) กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และเจ้าหน้าที่รักษาความปลอดภัย ต้องตรวจสอบผู้ติดต่อ อุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

๒) ผู้ใช้งานจะได้รับสิทธิ์ให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๓) หากบุคคลภายนอกขอเข้าใช้พื้นที่ที่ สพพ. ใช้บริการด้านสารสนเทศในพื้นที่ของหน่วยงานอื่น ให้ปฏิบัติตามระเบียบของหน่วยงานนั้นๆ

๔) หากบุคคลอื่นที่ไม่ได้รับการระบุสิทธิ์ผู้ใช้งานขอเข้าพื้นที่ หน่วยงานเจ้าของพื้นที่ ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต ทั้งนี้ หากได้รับอนุญาตจะต้องดำเนินการตามข้อ ๑, ๒ และ ๓

ส่วนที่ ๒
การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย
(Network System Control Room)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของ สพพ. โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่างๆ ที่มีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่าย

๒. คำจำกัดความของผู้เกี่ยวข้อง

๑) ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในห้องควบคุมระบบเครือข่าย

๒) เจ้าหน้าที่ หมายถึง เจ้าหน้าที่ สพพ. ที่มีสิทธิ์ในการเข้าออกอาคารสถานที่ ห้อง ตามที่กำหนดในทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่

๓) ผู้ติดต่อจากหน่วยงานภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่มาทำการติดต่อกับ สพพ.

๓. บทบาทและความรับผิดชอบ

๑) CIO (ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)

(๑.๑) อนุมัติสิทธิ์เข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

(๑.๒) อนุมัติกระบวนการควบคุมการเข้าออก ห้องควบคุมระบบเครือข่าย

๒) ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย

(๒.๑) ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในศูนย์ปฏิบัติการให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบเครือข่าย อย่างเคร่งครัด

(๒.๒) ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้าออกห้องควบคุมระบบเครือข่าย ต้องติดบัตรผู้ติดต่อ (Visitor) หรือบัตรประจาตัวขององค์กรนั้นๆ แล้ว เท่านั้น

๔. กระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

๑) ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย และเจ้าหน้าที่ สพพ. มีแนวทางปฏิบัติดังนี้

(๑.๑) ผู้ดูแลระบบห้องควบคุมระบบเครือข่าย ต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก “ทะเบียนผู้มีสิทธิ์เข้าออกพื้นที่” ได้แก่ เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูและระบบ (System Administrator) เป็นต้น

(๑.๒) สิทธิ์ในการเข้าออกห้องต่างๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคน ต้องได้รับการอนุมัติจาก CIO หรือผู้ที่ได้รับมอบหมาย เป็นลายลักษณ์อักษร โดยสิทธิ์ของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย

(๑.๓) เจ้าหน้าที่ทุกคนต้องลงบันทึกในกรณีเข้าออก เพื่อใช้ในการเข้าออกห้องควบคุมระบบเครือข่าย ตามกระบวนการที่ระบุในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

(๑.๔) ต้องจัดทำระบบเก็บบันทึกการเข้าออก สพพ. ตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

(๑.๕) กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่าย จะต้องมีการควบคุมอย่างรัดกุม

(๑.๖) การเข้าถึงห้องควบคุมระบบเครือข่าย ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

๒) ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

(๒.๑) ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการแลกบัตรที่ใช้ระบุตัวตน ได้แก่ บัตรประชาชน หรือใบอนุญาตขับขี่ กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ ‘Visitor’ แล้วทำการลงบันทึกข้อมูลลงในสมุดบันทึก ตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

(๒.๒) ผู้ติดต่อจากหน่วยงานภายนอก ที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายนอกองค์กร มาปฏิบัติงานที่ห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้าออกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่” ให้ถูกต้องชัดเจน

๓) ผู้ติดต่อจากหน่วยงานภายนอก ต้องติดบัตรผ่านในตำแหน่งที่สามารถเห็นได้ชัดเจนตลอดเวลา ที่อยู่ใน สพพ.

๔) เจ้าหน้าที่ ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการขออนุญาตเข้าออกกับเจ้าหน้าที่เป็นประจำทุกครั้ง

ส่วนที่ ๓
การควบคุมการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
(Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพพ. และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพพ. ได้อย่างถูกต้อง

๒. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

๑) ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญต้องมีการควบคุมการเข้าออกที่รัดกุม และอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์ และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

๒) ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓) ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูล และระบบข้อมูลได้

๔) ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สพพ. และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

๕) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๓. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control)

๑) สำนักงานกำหนดวัตถุประสงค์การใช้งานระบบเทคโนโลยีสารสนเทศแต่ละชนิด เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย โดยมีข้อปฏิบัติการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศที่เหมาะสม ดังนี้

(๑) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

(๒) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งาน ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสาร เพื่อขอสิทธิ์ในการเข้าสู่ระบบเฉพาะส่วนที่จำเป็น โดยคำนึงถึงประเภทข้อมูลและชั้นความลับ และกำหนดให้มีการอนุมัติเอกสารดังกล่าวโดย CIO ผู้อำนวยการสำนัก หรือผู้ที่ได้รับมอบหมาย เพื่อการจัดเก็บไว้เป็นหลักฐาน

(๓) เจ้าของข้อมูล และ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามภารกิจและการปฏิบัติงานในหน้าที่เท่านั้น เนื่องจากการใช้สิทธิ์เกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้น การกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

(๔) เจ้าของข้อมูล และ/หรือ เจ้าของระบบงาน จะต้องดำเนินการจัดทำแนวนโยบายและแนวปฏิบัติเกี่ยวกับข้อมูลสารสนเทศ และ/หรือ ระบบงานที่รับผิดชอบ เพื่อให้ผู้ใช้งานสามารถนำข้อมูลไปใช้หรือใช้ระบบงานได้อย่างถูกต้อง มีประสิทธิภาพ และเป็นมาตรฐานเดียวกัน

๒) กำหนดกฎเกณฑ์ในการอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ โดยกำหนดสิทธิ์ต่างๆ ให้แก่ผู้ใช้งานในแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่ สิทธิ์ในการอ่านอย่างเดียว สิทธิ์ในการสร้างข้อมูล สิทธิ์ในการป้อนข้อมูล สิทธิ์ในการแก้ไข สิทธิ์ในการอนุมัติ รวมถึงการไม่มีสิทธิ์ โดยผู้ใช้งานที่ต้องการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของ สพพ. จะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจาก CIO ผู้อำนวยการสำนัก หรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓) กำหนดสิทธิ์และมอบการใช้งานระบบเทคโนโลยีสารสนเทศแต่ละชนิด เพื่อควบคุมการอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศ โดยมีการแบ่งแยกอำนาจหน้าที่ของเจ้าหน้าที่ในส่วนของระบบเทคโนโลยีสารสนเทศ

(๑) มีหน่วยงานควบคุมการให้สิทธิ์การเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศให้สอดคล้องกับอำนาจหน้าที่และความจำเป็นของผู้ใช้งานอย่างเคร่งครัด

(๒) แบ่งแยกเจ้าหน้าที่ที่ปฏิบัติหน้าที่ในส่วนของการพัฒนาระบบเทคโนโลยีสารสนเทศ (Developer) ออกจากเจ้าหน้าที่ที่ทำหน้าที่บริหารระบบ (System Administrator) ที่ปฏิบัติอยู่ในส่วนคอมพิวเตอร์

(๓) กำหนดหน้าที่รับผิดชอบของงานในแต่ละหน้าที่ที่ปฏิบัติอยู่ในส่วนคอมพิวเตอร์อย่างชัดเจนเป็นลายลักษณ์อักษร

(๔) มีเจ้าหน้าที่สำรองในงานที่สำคัญ เพื่อทำงานทดแทนในกรณีจำเป็น ได้แก่ ผู้บริหารระบบเจห้าน้าที่ปฏิบัติการคอมพิวเตอร์ (Compute Operator) เป็นต้น

(๕) ให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจาก CIO ผู้อำนวยการสำนัก หรือผู้ที่ได้รับมอบหมาย เป็นลายลักษณ์อักษร

(๖) มีการตรวจสอบคุณสมบัติและอำนาจหน้าที่ของผู้ใช้งานอย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องยกเลิกหรือเปลี่ยนแปลงสิทธิ์ให้สอดคล้องกับระดับชั้นการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศทันที

(๗) จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญของผู้รับจ้างที่มาทำการบำรุงรักษาระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๘) ต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ โดยมีระบบเทคโนโลยีสารสนเทศที่สำคัญ ดังนี้

(๘.๑) ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application)

(๘.๒) ไปรษณีย์อิเล็กทรอนิกส์ (e-mail)

(๘.๓) ระบบอินเตอร์เน็ต

๔) กำหนดประเภทของข้อมูลที่กำหนดชั้นความลับ (Confidential Data and Information) ซึ่งเป็นข้อมูลที่มีความสำคัญและเป็นความลับ หากถูกเปิดเผยออกไปแล้วจะเกิดความเสียหาย หรือเกิดผลเสียอื่นๆ ต่อหน่วยงาน ต้องกำหนดประเภทของข้อมูล จัดแบ่งลำดับความสำคัญของข้อมูล จัดแบ่งลำดับขั้นความลับของข้อมูล จัดแบ่งระดับชั้นการเข้าถึง กำหนดเวลาเข้าถึงได้ และกำหนดช่องทางการเข้าถึงสำหรับระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัด ดังต่อไปนี้

(๑) กำหนดประเภทของข้อมูล ดังนี้

(๑.๑) ข้อมูลด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น

(๑.๒) ข้อมูลที่ให้บริการ ได้แก่ ข้อมูลด้านเศรษฐกิจ การเงิน และโครงการ เป็นต้น

(๒) จัดแบ่งลำดับความสำคัญของข้อมูล ดังนี้

(๒.๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด

(๒.๒) ข้อมูลที่มีระดับความสำคัญปานกลาง

(๒.๓) ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล ดังนี้

(๓.๑) กำหนดบุคคลผู้ทำหน้าที่เป็นผู้บริหารจัดการสารสนเทศภายในหน่วยงาน เป็นผู้ทำหน้าที่จัดหมวดสินทรัพย์สารสนเทศ ได้แก่ ข้อมูลดิจิตอล (Digital Data) หรือสารสนเทศดิจิทัล (Digital Information) โดยระบุชนิดลักษณะของข้อมูลให้ชัดเจนว่าเกี่ยวกับเรื่องใด (Topic) มีความสำคัญอย่างไร (Importance) และต้องมีการจัดลำดับชั้นความลับเป็นอย่างหนึ่งอย่างใดต่อไปนี้

(๓.๑.๑) “ชั้นลับที่สุด”

(๓.๑.๒) “ชั้นลับมาก”

(๓.๑.๓) “ชั้นลับ”

(๓.๑.๔) “ชั้นไม่ลับ หรือ ชั้นเปิดเผย”

กำหนดให้เจ้าหน้าที่ เป็นผู้ประสานกับผู้บริหารจัดการสารสนเทศภายในหน่วยงานในการจัดเก็บข้อมูลที่อยู่ในชั้นไม่ลับ หรือเปิดเผยนี้ เข้าสู่ระบบบริหารจัดการองค์ความรู้ (Knowledge Management System) หรือระบบจัดเก็บเอกสาร (Document Image System) ตามความเหมาะสม โดยให้ CIO ผู้อำนวยการสำนัก หรือผู้ที่ได้รับมอบหมาย พิจารณาอนุมัติในแบบฟอร์มการจัดเก็บสินทรัพย์สารสนเทศก่อนทุกครั้ง

(๓.๒) เอกสารหรือสิ่งตีพิมพ์ ที่พิมพ์หรือทำซ้ำขึ้นมาจากข้อมูลดิจิทัลหรือสารสนเทศดิจิทัล ซึ่งมีการกำหนดชั้นความลับไว้ ทั้งในกรณีทั้งหมดหรือบางส่วน ให้ถือว่ามีชั้นความลับเดียวกันกับข้อมูลดิจิทัลหรือสารสนเทศดิจิทัลนั้น ยกเว้นว่ามีการจัดลำดับชั้นความลับใหม่ โดยหน่วยงานผู้ผลิตเอกสารหรือสิ่งพิมพ์นั้น

(๓.๓) ให้บุคลากรเป็นผู้ประสานกับผู้บริหารจัดการสารสนเทศภายในหน่วยงานต้องทำการจัดหมวดหมู่ การกำหนดชั้นความลับ และการกำหนดระดับความสำคัญของเอกสาร เพื่อป้องกันสารสนเทศของ สพพ. ให้มีความปลอดภัยด้วยวิธีการที่เหมาะสม โดย สพพ. จัดให้มีกระบวนการในการจัดหมวดหมู่ของข้อมูลและสินทรัพย์สารสนเทศ กำหนดให้มีชั้นความลับที่สุด ชั้นลับมาก ชั้นลับ และชั้นไม่ลับ หรือ ชั้นเปิดเผย การกำหนดแนวทางการแบ่งชั้นความลับของข้อมูลของ สพพ. ต้องอยู่ในการควบคุมดูแลและรักษาความปลอดภัยที่เหมาะสมไม่ว่าจะอยู่ในรูปแบบใดก็ตาม มีการกำหนดชั้นความลับ โดยมีข้อพิจารณาดังนี้

(๓.๓.๑) ชั้นลับที่สุด กำหนดให้มีระดับความปลอดภัยที่ ๔ สำหรับข้อมูลและสารสนเทศที่มีความสำคัญต่อสำนักงานมากที่สุด ต้องได้รับการรักษาความลับของเนื้อหา โดยการเข้ารหัสอย่างยาก (Strong Encryption) และจำกัดการเข้าถึง (Access Control) เป็นอย่างดี ได้แก่ Private Key ของสำนักงาน หรือข้อมูลจากการประชุมที่มีมติที่ประชุมกำหนดให้เป็นชั้นความลับนี้ ตัวอย่างข้อมูลชั้นลับที่สุด ได้แก่ นโยบายหรือแผนการที่สำคัญยิ่งของสำนักงาน ซึ่งถ้าเปิดเผยก่อนเวลาอันสมควร อาจก่อให้เกิดผลเสียหายอย่างร้ายแรงแก่สำนักงาน แผนยุทธศาสตร์ที่เกี่ยวกับข้อมูลสำคัญในการปฏิบัติภารกิจของสำนักงานร่วมกับหน่วยงานอื่น เอกสารของสำนักงานที่เกี่ยวข้องกับความมั่นคงปลอดภัย เป็นต้น

(๓.๓.๒) ชั้นลับมาก กำหนดให้มีระดับความปลอดภัยที่ ๓ สำหรับข้อมูลและสารสนเทศที่มีความสำคัญต่อสำนักงานมาก ต้องได้รับการรักษาความลับของเนื้อหา โดยการเข้ารหัส (Encryption) หรือจำกัดการเข้าถึง (Access Control) ตัวอย่างข้อมูลลับมาก ได้แก่ รายงานเสนอการแต่งตั้งถอดถอนหรือโอนย้ายเจ้าหน้าที่ในตำแหน่งที่สำคัญมาก การเจรจาข้อตกลงที่สำคัญกับหน่วยงานอื่น เทคนิคที่ต้องอาศัยความชำนาญพิเศษ เป็นต้น

(๓.๓.๓) ชั้นลับ กำหนดให้มีระดับความปลอดภัยที่ ๒ สำหรับข้อมูลและสารสนเทศที่มีความสำคัญต่อสำนักงาน โดยการเข้ารหัสถึง (Strong Encryption) ตัวอย่างข้อมูลชั้นลับ ได้แก่ การดำเนินการที่เกี่ยวกับการเปลี่ยนแปลงตำแหน่งที่สำคัญในสำนักงาน ระเบียบวาระการประชุมลับ ประกาศหรือคำสั่งที่สำคัญที่อยู่ระหว่างการดำเนินการ เป็นต้น

(๓.๓.๔) ชั้นไม่ลับ หรือ ชั้นเปิดเผย กำหนดให้มีระดับความปลอดภัยที่ ๑ สำหรับข้อมูลและสารสนเทศที่ไม่มีความลับ สามารถเผยแพร่ได้ ตัวอย่างข้อมูลชั้นไม่ลับ หรือชั้นเปิดเผย ประกอบด้วยข้อมูลและสารสนเทศที่เป็นความรู้ของหน่วยงานในลักษณะงานโครงการ นโยบาย ข้อกฎหมาย พระราชบัญญัติ พระราชกฤษฎีกา พระราชกำหนด ข้อมูลและสารสนเทศที่เป็นประกาศ คำสั่งแต่งตั้ง ข่าวประชาสัมพันธ์

(๓.๔) ข้อมูลที่อยู่ในรูปแบบของเอกสารที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสม ตั้งแต่การเริ่มพิมพ์ การเก็บรักษา จนถึงการทำลายและกำหนดเป็นระเบียบปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ และลูกจ้างของสำนักงาน ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

(๔) จัดแบ่งระดับชั้นการเข้าถึง

(๔.๑) ผู้บริหารระบบ (Administrator) ต้องได้รับสิทธิ์ในการเข้าใช้งานจากฝ่ายสารสนเทศ โดยมีการกำหนด User และ Password ในการเข้าใช้งาน โดยผ่านทาง Active Directory (AD) ซึ่งแยกประเภทตามความรับผิดชอบ ได้แก่ Network, Admin, System Admin และ Database Admin เป็นต้น

(๔.๒) ผู้ใช้งาน ต้องได้รับสิทธิ์ในการเข้าใช้งานจากฝ่ายสารสนเทศ โดยต้องใช้งานผ่านระบบ Single Sign-On ของสำนักงาน และต้องใช้ User และ Password เป็นอย่างน้อย กรณีการเข้าถึงสารสนเทศหรือข้อมูลที่มีระดับความสำคัญมากที่สุด ต้องเพิ่มเติมอุปกรณ์พิสูจน์ตัวตน

(๕) กำหนดเวลาเข้าถึงได้

ตลอดเวลา ๒๔ ชั่วโมง ๗ วัน

(๖) กำหนดช่องทางการเข้าถึงสำหรับสารสนเทศอย่างเคร่งครัด

ผู้ได้รับสิทธิ์กทำการ Log In ด้วย User และ Password ผ่านระบบ Single Sign-On เป็นอย่างน้อย กรณีการเข้าถึงสารสนเทศหรือข้อมูลที่มีระดับความสำคัญมากที่สุด ต้องเพิ่มเติมอุปกรณ์พิสูจน์ตัวตน

๕) กำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ และสิทธิ์ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

(๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย

๔. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User Access) เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัย และผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๑) มีการกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training)

(๒) ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวัง หรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๓) จัดให้มีการฝึกอบรมการใช้งานระบบเทคโนโลยีสารสนเทศของ สพพ. อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการพัฒนาระบบเทคโนโลยีสารสนเทศขึ้นมาใช้งาน หรือมีการปรับปรุง/ปรับเปลี่ยนการใช้งานของระบบเทคโนโลยีสารสนเทศ

๒) การลงทะเบียนผู้ใช้งาน (User Registration)

ฝ่ายสารสนเทศ ซึ่งเป็นผู้ดูแลบริหารจัดการระบบ และมีหน้าที่ลงทะเบียนผู้ใช้งาน รวมถึงการตัดออกจากทะเบียนผู้ใช้งานทั่วไปและผู้ใช้งานระบบ กำหนดให้มีข้อปฏิบัติ ดังนี้

(๑) การลงทะเบียนผู้ใช้งานทั่วไป สำหรับระบบเทคโนโลยีสารสนเทศที่จำเป็นพื้นฐาน ซึ่งเป็นการใช้งานบนระบบอินทราเน็ต (Intranet) ได้แก่ ระบบการลงเวลาการปฏิบัติงาน ระบบบริหารการลาและการปฏิบัติงาน (Leave Management System) ระบบอิเล็กทรอนิกส์สำนักงาน (E-Office) ระบบบริหารเงินทุน (Capital Management System) ระบบบริหารทรัพยากรองค์กร (Enterprise Resource Planning) เป็นต้น รวมถึงการใช้งานบนระบบอินเทอร์เน็ต (Internet) ได้แก่ ระบบเว็บไซต์สำนักงาน ระบบไปรษณีย์อิเล็กทรอนิกส์ (e-Mail) เป็นต้น ฝ่ายสารสนเทศ ซึ่งเป็นผู้ดูแลบริหารจัดการระบบจะทำหน้าที่ประสานกับฝ่ายทรัพยากรบุคคล สำนักอำนวยการ เพื่อดำเนินการลงทะเบียนผู้ใช้งานทั่วไป

(๒) หากบุคลากรมีการโอน/ย้าย/ลาออก/สิ้นสุดการจ้าง หรือเมื่อเปลี่ยนตำแหน่งงานภายในหน่วยงาน หรือกรณีไปช่วยราชการที่อื่น ฝ่ายสารสนเทศจะทำหน้าที่ประสานกับฝ่ายทรัพยากรบุคคล สำนักอำนวยการ จะทำการระงับการใช้งานของรหัสผ่านทันที เมื่อบุคลากรพ้นจากภารกิจ รวมถึงทำการยกเลิกและตัดสิทธิ์การเข้าใช้งานระบบเทคโนโลยีสารสนเทศทุกระบบ พร้อมลบชื่อออกจากทะเบียนผู้ใช้งานทั่วไป และผู้ใช้งานระบบภายใน ๓๐ วัน ทั้งนี้ ภายหลังจากที่ได้รับแจ้งรายชื่อ ตำแหน่งและวันที่มีผลบังคับใช้ โดยมีหลักฐานเป็นลายลักษณ์อักษรจากฝ่ายทรัพยากรบุคคล สำนักอำนวยการ หรือหน่วยงานที่เกี่ยวข้องแล้ว

(๓) ฝ่ายสารสนเทศจะกำหนดรหัสชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในเบื้องต้น โดยใช้ข้อมูลจากส่วนกลางที่จัดเก็บใน Active Directory (AD) และส่งมอบให้แก่ผู้ใช้งาน ซึ่งระบบงานอนุญาตให้ผู้ใช้งานเปลี่ยนรหัสผ่านได้ด้วยตนเอง และหากมีปัญหา ได้แก่ ผู้ใช้งานลืมรหัสผ่าน เป็นฝ่ายสารสนเทศดำเนินการกำหนดรหัสผ่านใหม่ให้

๓) การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)

เป็นการกำหนดรายละเอียดที่เกี่ยวกับการกำหนดระดับสิทธิ์ การควบคุมและจำกัดสิทธิ์การใช้งานให้แก่ผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และความจำเป็นในการใช้งาน เพื่อให้สามารถเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงการมอบหมายสิทธิ์ สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นๆ ที่เกี่ยวข้องกับการเข้าถึง โดยมีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน

ฝ่ายสารสนเทศ ซึ่งเป็นผู้ดูแลบริหารจัดการระบบ และมีหน้าที่บริหารจัดการสิทธิ์ของผู้ใช้งาน โดยจัดให้มีการควบคุมและจำกัดสิทธิ์ เพื่อเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศ กำหนดให้มีข้อปฏิบัติดังนี้

(๑) กำหนดรหัสชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบตัวตนจริง และควบคุมการเข้าถึงข้อมูลในแต่ละชั้นความลับ โดยจำแนกผู้ใช้งานออกเป็นกลุ่มต่างๆ ตามระดับการใช้งานที่เหมาะสม โดยคำนึงถึงชั้นความลับของข้อมูล เพื่อกำหนดกลุ่มใช้งานและระดับการใช้ข้อมูลในการปฏิบัติงาน ได้แก่ กลุ่มผู้ใช้ที่มีสิทธิ์เข้าถึงระบบฐานข้อมูลและแฟ้มข้อมูล (Database and File System) กลุ่มผู้ใช้ที่มีสิทธิ์เข้าถึงเฉพาะข้อมูลสารสนเทศ รวมถึงผู้ใช้ระดับใดควรมีสิทธิ์แก้ไขข้อมูล ระดับใดควรสร้าง/ลบข้อมูลได้ และระดับใดสามารถเรียกดูข้อมูลได้เพียงอย่างเดียว เป็นต้น

(๒) กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้ หมายถึง ผู้ใช้ที่มีสิทธิ์สูงสุดนอกเหนือจากผู้ใช้ปกติ ได้แก่ ผู้ตรวจสอบภายใน เป็นต้น ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา และต้องได้รับความเห็นชอบ และอนุมัติจาก CIO ผู้อำนวยการสำนัก หรือผู้ที่ได้รับมอบหมาย นั้นๆ ก่อน

(๒.๑) ควบคุมการใช้งานอย่างเข้มงวด โดยกำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๒.๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

(๒.๓) มีการเปลี่ยนรหัสผ่านอย่างเคร่งครัดทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุกๆ ๓ เดือน เป็นต้น

(๓) ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

(๔) ระบบฐานข้อมูลที่สำคัญ ได้แก่ ระบบบริหารเงินทุน ระบบบริหารทรัพยากรบุคคล เป็นต้น ต้องสามารถบันทึกรายละเอียดเกี่ยวกับการเข้าถึง

๔) การบริหารจัดการบัญชีรายชื่อผู้ใช้งานงาน (User Account) และรหัสผ่านของเจ้าหน้าที่

(๑) ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้ง กำหนดสิทธิ์แยกตามหน้าที่ ที่รับผิดชอบซึ่งมีแนวทางปฏิบัติ ตามที่กำหนดไว้ในเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

(๒) การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตามเอกสาร “การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน”

(๓) กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน หมายถึง ผู้ใช้งานที่มีสิทธิ์สูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

(๓.๑) ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้นๆ

(๓.๒) ควรควบคุมการใช้งานอย่างเข้มงวด ได้แก่ กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๓.๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

(๓.๔) ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด ได้แก่ ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่าน ทุก ๓ เดือน เป็นต้น

๕) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

ฝ่ายสารสนเทศเป็นผู้บริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน โดยจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม และมีความมั่นคงปลอดภัย เนื่องจากรหัสผ่านเป็นวิธีพื้นฐานในการตรวจสอบตัวตนของผู้ใช้งานระบบ ดังนั้น จึงต้องมีการควบคุมที่เข้มงวด เพื่อให้มั่นใจว่าผู้ที่เข้ามาใช้ระบบนั้น คือบุคคลที่มีสิทธิ์เข้าสู่ระบบของสำนักงานอย่างแท้จริง กำหนดขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนมาใช้ระบบนั้น

(๑) รหัสผ่านชั่วคราวจะมีการนำมาใช้สำหรับผู้ใช้ที่ลืมรหัสผ่านและมีหลักฐานพิสูจน์ตัวตนได้ว่าเป็นผู้ใช้ที่มีสิทธิ์ใช้งานระบบได้ ได้แก่ มีรายชื่อในระบบ Active Directory (AD) เป็นต้น

(๒) แสดงรหัสผ่านในรูปของสัญลักษณ์ หรือตัวอักษร “x” หรือ “๐” ในขณะพิมพ์รหัสผ่านแต่ละตัวอักษร โดยต้องไม่ปรากฏหรือแสดงรหัสผ่านที่แท้จริงออกมา

(๓) การตั้งรหัสผ่านต้องไม่ใช้ข้อมูลที่เกี่ยวข้องกับสำนักงาน หรือเป็นข้อมูลส่วนตัวของผู้ใช้งาน ซึ่งง่ายแก่การคาดเดา ได้แก่ เลขที่บัตรประชาชน เลขที่บัตรประกันสังคม รหัสบัตรต่างๆ ที่อยู่ หมายเลขโทรศัพท์ ชื่อบุคคลในครอบครัว เป็นต้น รวมถึงต้องไม่ใช้ศัพท์ที่มาจากพจนานุกรม ชื่อภาพยนตร์ ชื่อสถานที่หรือชื่อสิ่งลึกลับ เพราะศัพท์ต่างๆ เหล่านี้ ง่ายต่อการคาดเดาของผู้โจมตีระบบ (Hackers)

(๔) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนอัตโนมัติ (Save Password) สำหรับเครื่องคอมพิวเตอร์ที่เจ้าหน้าที่ครอบครองอยู่ รวมถึงไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตของบุคคลอื่น

(๕) กำหนดวิธีการส่งมอบรหัสผ่านให้แก่ผู้ใช้งานอย่างรัดกุมและปลอดภัย ได้แก่ การใส่ซองปิดผนึก การส่งทางไปรษณีย์อิเล็กทรอนิกส์ (e-Mail) และบังคับให้ใส่วัน เดือน ปีเกิด ในการเปิดอ่านไปรษณีย์อิเล็กทรอกนิกส์ เป็นต้น และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(๖) การตั้งรหัสผ่าน (Password) ควรมีส่วนประกอบของอักษร อักขระพิเศษ และ/หรือ ตัวเลขที่ประสมกัน ตามลักษณะดังต่อไปนี้

- ความยาวไม่น้อยกว่า ๘ ตัวอักษร
- อักษรตัวพิมพ์ใหญ่ ได้แก่ A, B, C,... เป็นต้น
- อักษรตัวพิมพ์เล็ก ได้แก่ a, b, c,... เป็นต้น
- ตัวเลข ได้แก่ ๐, ๑, ๒,... เป็นต้น
- สัญลักษณ์พิเศษ ได้แก่ !, @, #, $,... เป็นต้น

(๗) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๘) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ ไม่เกิน ๓ ครั้ง

(๙) รหัสผ่านเข้าระบบบริหารจัดการด้านเครือข่ายและระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ การเข้า Root, Enable, NT Admin, Application Admin Account เป็นต้น จะต้องมีการเปลี่ยนรหัสผ่านเป็นประจำอย่างน้อยทุก ๓ เดือน

(๑๐) รหัสผ่านของผู้ใช้งาน ได้แก่ e-Mail, Website, Desktop Computer, Notebook, ระบบเทคโนโลยีสารสนเทศ เป็นต้น ต้องเปลี่ยนเป็นประจำอย่างน้อยทุก ๖ เดือน ทั้งนี้ แนะนำให้เปลี่ยนเป็นประจำทุก ๓ เดือน จะสร้างความปลอดภัยได้ดียิ่งขึ้น

(๑๑) ไม่อนุญาตให้เจ้าหน้าที่ใช้รหัสผ่านร่วมกัน ถ้ารหัสผ่านถูกเปิดเผยต้องเปลี่ยนรหัสผ่านใหม่ โดยทันที

(๑๒) ผู้ใช้งานไม่ควรเปลี่ยนรหัสผ่านของผู้อื่น ยกเว้นผู้มีหน้าที่ในการบริหารจัดการรายชื่อผู้ใช้งานและรหัสผ่านเท่านั้น

๖) การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review Of User Access Rights)

(๑) เจ้าของข้อมูล จะต้องมีการทบทวนสิทธิ์การเข้าใช้งานและสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งานและปรับปรุงบัญชีผู้ใช้งานให้มีความเหมาะสมอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด ทุกๆ ๖ เดือน หรืออย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับเปลี่ยนเคลื่อนย้ายบุคลากร ได้แก่ การโอน/ย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ ลาออก สิ้นสุด/ยกเลิกการจ้าง เป็นต้น เพื่อให้มั่นใจได้ว่าสิทธิ์ต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๒) การให้อำนาจสำหรับสิทธิ์การเข้าถึงพิเศษ ต้องทบทวนบ่อยกว่าปกติ โดยทำทุกๆ ๓ เดือน

(๓) การจัดสรรสิทธิ์พิเศษ ต้องได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เพื่อให้มั่นใจได้ว่าไม่มีการได้สิทธิ์พิเศษกับผู้ใช้ที่ไม่ได้รับมอบอำนาจ

(๔) การเปลี่ยนแปลงของผู้ใช้ที่ได้รับสิทธิ์พิเศษ ต้องถูกบันทึกเพื่อการทบทวน

(๕) กรณีมีปัญหาการใช้หรือนำระบบงานไปปฏิบัติโดยไม่ได้รับอนุญาต ฝ่ายสารสนเทศจำดำเนินการติดตาม ตรวจสอบ และทบทวนการใช้งาน หากมีผลที่คาดว่าจะกระทบถึงระบบงานในอนาคต ฝ่ายอาจพิจารณายกเลิกการใช้งานนั้น

๕. การบริหารจัดการการเข้าถึงระบบเครือข่าย (Network Access Control)

๑) ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้งาน และกลุ่มของระบบเทคโนโลยีสารสนเทศ ได้แก่ โซนภายใน (Internal zone) โซนภายนอก (External zone) เป็นต้น เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๒) ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๓) ผู้ดูแลระบบ ควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๔) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕) การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๖) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการภายใต้การควบคุมของเจ้าหน้าที่สารสนเทศเท่านั้น

๗) ใช้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อควบคุมและติดตามผู้ใช้งานระบบ ดังนี้

(๗.๑) กำหนดให้ผู้ดูแลระบบเครือข่ายมีหน้าที่ความรับผิดชอบในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) ลงบนสื่อเก็บข้อมูลที่รักษาความครบถ้วน ถูกต้อง แท้จริง โดยข้อมูลสามารถระบุถึงตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ โดยกำหนดชั้นความลับในการเข้าถึงข้อมูล เพื่อป้องกันและจำกัดสิทธิ์การเข้าถึงเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ห้ามแก้ไขหรือเปลี่ยนแปลงข้อมูลเก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของ สพพ. (Internal IT Auditor) หรือบุคคลที่ สพพ. มอบหมาย

(๗.๒) บันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

(๗.๓) ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

๘) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้วิธีการระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๘.๑) การนำอุปกรณ์เครือข่ายมาเชื่อมต่อกับเครือข่ายของ สพพ. ต้องได้รับอนุญาตจากฝ่ายสารสนเทศก่อน จึงจะสามารถดำเนินการได้

(๘.๒) ผู้ดูแลระบบเครือข่ายมีหน้าที่ในการเชื่อมต่อสัญญาณที่ได้รับอนุญาตและให้สิทธิ์ ในการเชื่อมต่อตามที่ฝ่ายสารสนเทศกำหนด และสามารถระงับสัญญาณการเชื่อมต่อได้เมื่อสิ้นสุดการอนุญาต

(๘.๓) จะต้องมีการจำกัดสิทธิ์การเข้าใช้อุปกรณ์ได้ โดยให้มีการกำหนดวิธีการพิสูจน์ ตัวตนในการเข้าใช้งานอุปกรณ์โดยใช้ Username Password หมายเลข MAC Address เพื่อความปลอดภัยและเหมาะสมในการเข้าถึง

๙) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ผู้ใช้ระบบทุกคน เมื่อจะเข้าใช้งานระบบของสำนักงาน มีแนวทางปฏิบัติ ดังนี้

(๙.๑) กำหนดขั้นตอนปฏิบัติสำหรับการบริหารจัดการบัญชีผู้ใช้งานที่อนุญาตให้สามารถเข้าใช้ระบบเทคโนโลยีสารสนเทศจากระยะไกล

(๙.๒) การแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username)

(๙.๓) การพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน

(๙.๔) การเข้าสู่ระบบเทคโนโลยีสารสนเทศของสำนักงานจากระบบอินเทอร์เน็ตนั้น ต้องได้รับอนุญาตจากฝ่ายสารสนเทศ

(๙.๕) การใช้งานระบบอินเทอร์เน็ต เพื่อเข้ามายังระบบเทคโนโลยีสารสนเทศของสำนักงาน ต้องมีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ SSL หรือ VPN เป็นต้น

(๙.๖) กำหนดมาตรการพิเศษ เพื่อป้องกันความลับและความถูกต้องของข้อมูลสำคัญ เมื่อต้องส่งผ่านข้อมูลนั้นทางเครือข่ายสาธารณะ หรือเครือข่ายระบบอินเทอร์เน็ต หรือเครือข่ายไร้สาย

(๙.๗) กำหนดมาตรการพิเศษ เพื่อป้องกันระบบเทคโนโลยีสารสนเทศที่มีการเชื่อมโยงกับเครือข่ายสาธารณะ

(๙.๘) กำหนดมาตรการพิเศษ เพื่อเฝ้าระวังสภาพความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศต่างๆ เพื่อให้สามารถใช้งานได้อย่างเนื่อง

๑๐) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) เพื่อควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพ และทางเครือข่าย มีข้อปฏิบัติ ดังนี้

(๑๐.๑) มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของ สพพ. ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

(๑๐.๒) IP address ของระบบงานเครือข่ายภายในของ สพพ. จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบของ ฝ่ายสารสนเทศได้โดยง่าย

(๑๐.๓) หากผู้บริหารระบบ (Administrator) จำเป็นต้องใช้งานผ่านพอร์ต ต้องได้รับอนุญาตจากฝ่ายสารสนเทศ

(๑๐.๔) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ สำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(๑๐.๕) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

(๑๐.๖) ปิดการใช้งาน เพื่อป้องกันพอร์ตที่ไม่มีการใช้งาน

(๑๐.๗) ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัด ระยะเวลาเท่าที่จำเป็น โดยต้องได้รับอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๑๑) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) เพื่อควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน หรือเชื่อมต่อระหว่างหน่วยงาน มีข้อปฏิบัติ ดังนี้

(๑๑.๑) ระบบเครือข่ายทั้งหมดของ สพพ. ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอก สพพ. ควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุรุก หรือโปรแกรมในการทำ Packet filtering ได้แก่ การใช้ไฟร์วอล (Firewall) หรือฮาร์ดแวร์ (Hardware) อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

(๑๑.๒) ให้ผู้ดูแลระบบกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัย ได้แก่ Firewall และ IPS/IDS เป็นต้น

(๑๑.๓) การควบคุมการเข้าถึงระบบเครือข่ายภายในของสำนักงาน

(๑๑.๓.๑) การเข้าสู่ระบบเครือข่ายของสำนักงาน โดยผ่านทางระบบอินเทอร์เน็ตจะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจาก CIO ผู้อำนวยการสำนัก หรือผู้ที่ได้รับมอบหมาย ก่อนที่จะสามารถใช้งานได้ทุกกรณี

(๑๑.๓.๒) การเข้าสู่ระบบงานเครือข่ายภายใน สพพ. โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการล๊อกอิน เพื่อต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) และตรวจสอบความถูกต้อง

๑๒) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) เพื่อควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์ และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ มีข้อปฏิบัติ ดังนี้

(๑๒.๑) กำหนดให้ผู้ดูแลระบบเครือข่ายเป็นผู้บริหารจัดการสิทธิ์ให้แก่ผู้ใช้งานในการเข้าถึงระบบเครือข่ายและใช้งานทรัพยากรเครือข่าย เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๑๒.๒) ผู้ใช้งานมีสิทธิ์ในการเข้าถึงระบบเครือข่ายและใช้งานทรัพยากรเครือข่ายตามสิทธิ์ที่ได้รับอนุญาตตามภารกิจหน้าที่ขอตนเองเท่านั้น

(๑๒.๓) กำหนดหมายเลขเครือข่าย (IP Address) สำหรับเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องคอมพิวเตอร์แมม่ข่าย เพื่อแสดงตัวตนและควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของ

คอมพิวเตอร์และการส่งผ่านหรือไหลเวียนข้อมูลหรือสารสนทเศสอดคล้องข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ โดยผู้ใช้งานต้องทำการพิสูจน์ตัวตนก่อนการเข้าใช้งานระบบเครือข่ายทุกครั้ง และห้ามมิให้เปิดเผยหมายเลขเครือข่าย (IP Address) แก่บุคคลที่ไม่มีหน้าที่เกี่ยวข้องกับการใช้หมายเลขเครือข่ายดังกล่าว

(๑๒.๔) กำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

(๑๒.๕) บริหารจัดการระบบเครือข่ายโดยการแปลงหมายเลขเครือข่าย เพื่อแบ่งแยกเครือข่ายย่อย เพื่อจำกัดสิทธิ์ใช้งานระบบเครือข่ายร่วมกันภายในหน่วยงาน (สำนัก/ฝ่าย) ที่มีภารกิจหน้าที่เดียวกัน ได้แก่ การแชร์ไฟล์ แชร์เครื่องพิมพ์จากเครือข่าย เป็นต้น

(๑๒.๖) ระบบเครือข่ายที่มีความจำเป็นต้องเชื่อมต่อไปยังเครือข่ายภายนอกสำนักงานจะต้องทำการเชื่อมต่อกับอุปกรณ์รักษาความปลอดภัย (Firewall) และติดตั้งระบบป้องกันการรุกราน (Intrusion Prevention System : IPS)

(๑๒.๗) ห้ามผู้ใช้งานนำอุปกรณ์เครือข่ายมาติดตั้ง โดยมิได้รับอนุญาตจาก CIO หรือผู้อำนวยการสำนัก หรือผู้ที่ได้รับมอบหมาย

(๑๒.๘) กำหนดมาตรการบังคับใช้เส้นทางเครือข่าย (Enforced path) จากเครื่องคอมพิวเตอร์ลูกข่าย ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อจำกัดเส้นทางบนเครือข่ายโดยทำการเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ เพื่อควบคุมการเข้าใช้งานระบบเครือข่ายจากภายนอก มีข้อปฏิบัติ ดังนี้

(๑๒.๘.๑) การเข้าสู่ระบบเครือข่ายจากระยะไกล (Remote Access) ให้ใช้มาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน โดยต้องมีการควบคุมอย่างเข้มงวด และต้องได้รับการอนุมัติใช้ระบบเครือขายจากระยะไกลจาก CIO ผู้อำนวยการสำนัก หรือผู้ที่ได้รับมอบหมาย

(๑๒.๘.๒) การให้สิทธิ์ในการเข้าสู่ระบบเครือข่ายจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานพร้อมระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสำนักงานอย่างเพียงพอ และต้องได้รับอนุมัติใช้ระบบเครือข่ายจากระยะไกลจาก CIO ผู้อำนวยการสำนัก หรือผู้ที่ได้รับมอบหมายจากสำนักงานก่อนทุกครั้ง

(๑๒.๘.๓) ควบคุมพอร์ต (Port) ที่ใช้เชื่อมต่อเข้าสู่ระบบเครือข่ายอย่างรัดกุม ไม่เปิด Port ทิ้งไว้โดยไม่จำเป็น และให้ตัดการเชื่อมต่อเมื่อไม่ได้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๑๓) การแบ่งแยกระบบเครือข่าย (Segregation in Networks)

มีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบเทคโนโลยีสารสนเทศ เพื่ออำนวยความสะดวกในการควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ ดังนี้

(๑๓.๑) เครือข่ายภายนอก

(๑๓.๒) เครือข่ายภายในสำนักงาน

(๑๓.๓) เครือข่ายไร้สาย

๖. การบริหารจัดการการเข้าถึงระบบคอมพิวเตอร์แม่ข่าย

๑) กำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่าย และระบบเทคโนโลยีสารสนเทศของหน่วยงานได้

๓) มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่า มีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ ผู้ดูแลระบบจะต้องมีการรายงาน CIO และดำเนินการแก้ไขโดยทันที

๔) ผู้ดูแลระบบ และบุคคลที่ได้รับอนุญาตสามารถเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น ได้แก่ Telnet ftp หรือ ping เป็นต้น ทั้งนี้ หากมีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการเพิ่มเติมด้วย

๕) ติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ ได้แก่ web server เป็นต้น

๖) มีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไข หรือบำรุงรักษา

๗) การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการภายใต้การควบคุมของฝ่ายสารสนเทศ เท่านั้น

๘) ผู้ดูแลระบบ (System Administrator) ทำหน้าที่บริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

๙) มีการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) เพื่อควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพ และทางเครือข่าย

๑๐) กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

(๑๐.๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของ สพพ. จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจาก CIO ผู้อำนวยการสำนัก หรือผู้ที่ได้รับมอบหมาย

(๑๐.๒) ผู้ดูแลระบบได้ควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

(๑๐.๓) วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจาก CIO ผู้อำนวยการสำนัก หรือผู้ที่ได้รับมอบหมาย

(๑๐.๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือ ความจำเป็นในการดำเนินงานกับ CIO ผู้อำนวยการสำนัก หรือผู้ที่ได้รับมอบหมาย

(๑๐.๕) การเข้าใช้งานต้องผ่านระบบการพิสูจน์ตัวตนจากระบบของ สพพ.

๗. การบริหารจัดการการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

ฝ่ายสารสนเทศได้กำหนดมาตรการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของ สพพ. ในขณะที่ไม่มีผู้ดูแล ดังต่อไปนี้

๑) ผู้ใช้งานต้องออกจาก (Log out) ระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อเสร็จสิ้นการใช้งานหรือไม่อยู่ ที่หน้าจอเป็นเวลานานๆ

๒) ป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตน

๓) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกันการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

๔) เมื่อผู้ใช้งานระบบเทคโนโลยีสารสนเทศทิ้งไว้โดยไม่ใช้งานเป็นเวลานาน ระบบจะยุติการใช้งานระบบ ภายในระยะเวลา ๑๐ นาที หรือตามความเหมาะสมขึ้นอยู่กับระบบนั้นๆ

๘. การบริหารจัดการการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ผู้ดูแลระบบ (System Administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Controller) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของสำนักงาน จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้ กำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน เพื่อเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสำนักงาน โดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย กำหนดการควบคุมการเข้าถึงระบบปฏิบัติการ มีข้อปฏิบัติ ดังนี้

๑) <u>การควบคุมการเข้าถึงระบบปฏิบัติการ</u>

กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการต้องควบคุม โดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๑) เมื่อฝ่ายสารสนเทศ ได้รับการแจ้งผ่านทางจดหมายอิเล็กทรอนิกส์จาก ฝ่ายบุคคลตามกระบวนการเพื่อจัดหาเครื่องคอมพิวเตอร์ให้กับเจ้าหน้าที่หรือลูกจ้าง ที่รับใหม่ ฝ่ายสารสนเทศจะทำการสร้างชื่อผู้ใช้งานงาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ สพพ. ซึ่งเป็นระบบ Active Directory หลังจากนั้นผู้ใช้งานงานต้องทำการเปลี่ยนรหัสผ่าน (Password) เมื่อทำการลงชื่อเข้า (Login) ครั้งแรก

(๒) ผู้ใช้งานงานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตน ในการเข้าใช้งานเครื่องคอมพิวเตอร์ของ สพพ.

(๓) ผู้ใช้งานงานควรทำการลงบันทึกออก (Logout) ทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานกว่า ๓๐ นาที

๒) <u>การระบุและยืนยันตัวตนของผู้ใช้งาน</u> (User Identification and Authentication)

กำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตันของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง มีข้อปฏิบัติ ดังนี้

(๒.๑) การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยจะทำการเก็บข้อมูลการทางจราจรคอมพิวเตอร์ (Log) ในกรณีนี้ สพพ. ได้ใช้ระบบ Active Directory เป็นตัวควบคุม

(๒.๒) การแสดงตัวตน (Identification) ด้วยผู้ใช้ (Username)

(๒.๓) การพิสูจน์ตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password) โดยระบบ Active Directory มีการจำกัดระยะเวลาในการป้อนรหัสผ่าน และสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๓) การบริหารจัดการรหัสผ่าน (Password Management System)

มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ มีข้อปฏิบัติ ดังนี้

(๓.๑) ฝ่ายสารสนเทศจะทำการสร้างชื่อผู้ใช้งานงาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งาน โดยระบบ Active Directory

(๓.๒) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านของตนเองในครั้งแรกที่มีการเข้าสู่ระบบ และให้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ที่ได้กำหนดไว้

๔) การใช้งานโปรแกรมอรรถประโยชน์ (User of System Utilities)

เพื่อป้องกันการละเมิดลิขสิทธิ์หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว เนื่องจากการใช้งานซอฟต์แวร์ที่ได้มาจากแหล่งภายนอกหรือโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ และมีความเสี่ยงในการใช้งานโปรแกรมไม่ประสงค์ดี จึงต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ มีข้อปฏิบัติ ดังนี้

(๔.๑) จำกัดสิทธิ์การเข้าถึง และกำหนดสิทธิ์อย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๔.๒) อนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้ง

(๔.๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก หากไม่ได้ใช้งานเป็นประจำ

(๔.๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๔.๕) มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๔.๖) ห้ามติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอกสำนักงานที่ไม่มีลิขสิทธิ์ รวมทั้งการใช้ไฟล์อื่นๆ ที่ไม่อนุญาตให้ใช้งาน

(๔.๗) ให้มีการตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

(๔.๘) ให้ติดตั้งซอฟต์แวร์ เพื่อป้องกันโปรแกรมไม่ประสงค์ดีให้กับระบบเทคโนโลยีสารสนเทศ

(๔.๙) กำหนดหน้าที่ความรับผิดชอบ ขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่พบ

(๔.๑๐) มีการติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

(๔.๑๑) ให้มีการสร้างความตระหนักเกี่ยวโปรแกรมไม่ประสงค์ดี เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๕) การกำหนดระยะเวลาเพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน (Session Time-out)

(๕.๑) ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบเทคโนโลยีสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาที เป็นอย่างน้อย หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบ เมื่อว่างเว้นจากการใช้งานให้สั้นขึ้นหรือเป็นเวลา ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญ

(๕.๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศ ระบบงาน อุปกรณ์เครือข่าย มีการยกเลิก และหมดเวลาการใช้งาน รวมทั้งปิดการใช้งานด้วย หลังจากที่ไม่มีกิจกรรมใช้งานช่วงระยะเวลาหนึ่งที่กำหนดไว้

(๕.๓) กำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง โดยเฉพาะระบบงานที่มีข้อมูลสำคัญ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๕.๔) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์ และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๕.๕) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติหลังจากที่มีไม่การใช้งานเป็นระยะเวลาตามที่กำหนด

๖) การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบเทคโนโลยีสารสนเทศ หรือโปรแกรมที่มีความเสี่ยง หรือมีความสำคัญสูง มีข้อปฏิบัติ ดังนี้

(๖.๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศสำหรับระบบเทคโนโลยีสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ ๔ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง หรือกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของสำนักงานตามปกติเท่านั้น และกำหนดให้ระบบยกเลิกการเชื่อมต่อหากผู้ใช้งานไม่มีการใช้งานเกิน ๓๐ นาที

(๖.๒) กำหนดให้ระบบเทคโนโลยีสารสนเทศ หรือระบบงานที่มีความสำคัญสูง หรือระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน) มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

(๖.๓) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๙. การบริหารจัดการการใช้งานบัญชีผู้ใช้งาน (Account)

๑) ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้งาน (Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้งาน (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๒) ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้งาน (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอนจำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจาก ผู้บังคับบัญชา

๓) ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้งาน (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๑๐. การบริหารจัดการการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) หรือควบคุมการเข้าถึงการใช้งานของผู้ใช้งานงานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน โดยหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้ ดังนี้

(๑.๑) กำหนดประเภทของข้อมูลและสารสนเทศตามแนวทางปฏิบัติ ข้อ ๓ การเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

(๑.๒) ขั้นตอนปฏิบัติเพื่อการจัดการกับข้อมูลตามระดับชั้นความลับต้องประกอบด้วยวิธีการประมวลผลการควบคุมการเข้าถึง การจัดเก็บ การจัดการกับสื่อบันทึกข้อมูล การทำป้ายบ่งชี้ และการสื่อสารข้อมูลอย่างมั่นคงปลอดภัย

(๑.๓) ให้มีการจำกัดการเข้าถึงข้อมูลสำคัญ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๑.๔) มีมาตรการเพื่อตรวจสอบว่าข้อมูลที่นำออกจากระบบงานมีความถูกต้องและสมบูรณ์ก่อนที่จะนำไปใช้งานต่อไป

(๑.๕) มีความตระหนัก และมาตรการป้องกันข้อมูลสำคัญที่มีการสั่งพิมพ์ออกมาทางเครื่องพิมพ์ เพื่อป้องกันการเข้าถึงโดยผู้อื่น

(๑.๖) จัดทำบัญชีรายชื่อผู้มีสิทธิ์เข้าถึงข้อมูลและสื่อบันทึกข้อมูลและสื่อบันทึกข้อมูลสำคัญและมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ

๒) <u>การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ</u> (Security of System Documentation)

(๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ โดยผู้เป็นเจ้าของระบบนั้น

(๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ (อินเทอร์เน็ต) เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

๓) <u>การพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก</u>

(๑) ควรจัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

(๒) ให้ระบุว่าใครจะเป็นผู้มีสิทธิ์ในสินทรัพย์ทางปัญญาสำหรับ Source Code ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างหรือผู้ให้บริการภายนอก

(๓) ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๔) <u>มาตรการควบคุมผู้ให้บริการภายนอก</u> (Outsource) กรณีมีการว่าจ้างเหมาผู้ให้บริการภายนอกเข้ามาดำเนินการพัฒนา บำรุงรักษาระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายของสำนักงาน กำหนดมาตรการควบคุม ดังนี้

(๑) การคัดเลือกผู้ให้บริการภายนอก

(๑.๑) กำหนดเกณฑ์ในการคัดเลือกผู้ให้บริการภายนอก และคัดเลือกผู้ให้บริการภายนอกที่มีขั้นตอนการปฏิบัติงานที่รอบคอบ รัดกุม และเป็นที่น่าเชื่อถือ

(๑.๒) สัญญาต้องระบุเกี่ยวกับการรักษาความลับของข้อมูล (Data Confidentiality) และขอบเขตของงานและเงื่อนไขในการให้บริการ (Service Level Agreement) อย่างชัดเจน

(๒) การควบคุมผู้ให้บริการภายนอก

(๒.๑) ผู้ให้บริการภายนอกที่ต้องการสิทธิ์ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักงาน ต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจาก CIO หรือผู้ที่ได้รับมอบหมาย

(๒.๒) กรณีที่ใช้บริการด้านการพัฒนาระบบงาน กำหนดให้ผู้ให้บริการภายนอกเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบ (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการภายนอกอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้ โดยให้เจ้าหน้าที่ควบคุมดูแลการทำงานของผู้ให้บริการภายนอกอย่างใกล้ชิดในกรณีที่ผู้ให้บริการภายนอกมาปฏิบัติหน้าที่ที่สำนักงาน (Onsite Service) และให้เจ้าหน้าที่ตรวจสอบการทำงานของผู้ให้บริการภายนอกอย่างละเอียดในกรณีที่เป็นการบริการในลักษณะ Remote Access และปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกล (Modem) ทันทีที่การให้บริการเสร็จสิ้น

(๒.๓) การอนุญาตให้ผู้ให้บริการภายนอกเข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกล (Modem) ที่ใช้ทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวจะตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานและจะเปิดให้ใช้ได้ เมื่อมีการร้องขอเท่าที่จำเป็น

(๒.๔) ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบงานของผู้ให้บริการภายนอกที่สิ้นสุดการว่าจ้าง/เปลี่ยนการจ้างงาน โดยทันที ภายในระยะเวลาที่กำหนดไว้

(๒.๕) ดำเนินการเพิกถอน ลบ หรือเปลี่ยนรหัสปผ่านของผู้ให้บริการภายนอกที่สิ้นสุดการว่าจ้าง/เปลี่ยนการจ้างงานโดยทันที หรือภายในระยะเวลาที่กำหนดไว้

(๒.๖) ดำเนินการลยหรือเปลี่ยนชื่อของผู้ให้บริการภายนอกที่สิ้นสุดการว่าจ้าง/เปลี่ยนการจ้างงาน ออกจากเอกสารต่างๆ ของสำนักงานที่มีชื่อของบุคคลดังกล่าวอยู่ในนั้น

(๒.๗) ดำเนินการให้ผู้ให้บริการภายนอกจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ

(๒.๘) กำหนดให้ผู้ให้บริการภายนอกรายงานการปฏิบัติงาน ปัญหาต่างๆ ที่เกิดขึ้น หรือมีโอกาสที่จะเกิดขึ้นได้ พร้อมแนวทางแก้ไข

(๒.๙) มีขั้นตอนในการตรวจรับงานของผู้ให้บริการภายนอก

๕) <u>การบริหารจัดการกับระบบซึ่งไวต่อการรบกวน</u>

ระบบซึ่งไวต่อการรบกวน ระบบที่มีผลกระทบ และมีความสำคัญสูงต่อสำนักงาน ได้แก่ ระบบสารสนเทศด้านบริหารเงินทุน ระบบบริหารทรัพยากรบุคคล และระบบบัญชีและการเงิน เป็นต้น ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ และหากจำเป็นต้องมีการใช้งานผ่านเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ต่างๆ ต้องมีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเครลื่อนที่ต่างๆ รวมถึงการปฏิบัติงานจากภายนอกสนกงาน (Mobile Computing and Teleworking) มีข้อปฏิบัติ ดังนี้

(๑) จัดให้มีการบริหารจัดการสภาพแวดล้อมในส่วนของพื้นที่ห้องปฏิบัติการคอมพิวเตอร์ ดังนี้

(๑.๑) กำหนดระเบียบหรือแนวทางปฏิบัติในการเข้า-ออกพื้นที่ห้องปฏิบัติการคอมพิวเตอร์

(๑.๒) ควบคุมการเข้า-ออก ด้วยระบบ Hand Scan และระบบ Finger Print พร้อมระบบ CCTV

(๑.๓) ติดตั้งระบบสำรองกระแสไฟฟ้า (UPS)

(๑.๔) จัดหาเครื่องกำเนิดกระแสไฟฟ้า (Generator)

(๑.๕) ติดตั้งระบบระบายอากาศ

(๑.๖) ติดตั้งระบบปรับอากาศ และควบคุมความชื้น

(๑.๗) ติดตั้งระบบดับเพลิง ระบบตรวจสอบควันไฟและน้ำรั่วซึม

(๒) มีการสำรองข้อมูลและกู้คืนระบบเทคโนโลยีสารสนเทศ (Backup And Recovery) ระบุไว้ในแผนสำรองข้อมูลและระบบสารสนเทศ

(๓) มีแผนฉุกเฉิน กรณีระบบคอมพิวเตอร์ขัดข้อง ระบุไว้ในแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน (IT Contingency Plan)

(๔) มีแผนฉุกเฉิน กรณีเกิดอุทกภัย หรือภัยพิบัติธรรมชาติ ระบุไว้ในแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน (IT Contingency Plan)

(๕) ในระบบที่มีผลกระทบและความสำคัญสูงต่อสำนักงาน หากต้องมีการใช้งานผ่านเครื่องคอมพิวเตอร์หรืออุปกรณ์สื่อสารเคลื่อนที่ต่างๆ ซึ่งมิใช่สินทรัพย์ของสำนักงานต้องได้รับอนุญาตจากฝ่ายสารสนเทศ

๖) <u>การควบคุมคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่</u> (Mobile Computing and Teleworking)

กำหนดข้อปฏิบัติและมาตรการที่เหมาะสม เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และเครื่องมือสื่อสารเคลื่อนที่ รวมถึงการดูแลรักษาความปลอดภัยในการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ ดังนี้

(๑) <u>การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล</u> (User of Personal Computer)

(๑.๑) <u>แนวทางปฏิบัติในการใช้งานทั่วไป</u>

(๑.๑.๑) เครื่องคอมพิวเตอร์ที่สำนักงาน อนุญาตให้ผู้ใช้ใช้งานเป็นสินทรัพย์ของสำนักงาน ดังนั้น ผู้ใช้งานจึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ เพื่องานของสำนักงาน

(๑.๑.๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของสำนักงาน ต้องเป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์มาอย่างถูกกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว แก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๑.๑.๓) ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของสำนักงาน

(๑.๑.๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการ โดยเจ้าหน้าที่ของฝ่ายสารสนเทศ หรือผู้รับบริการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับสำนักงานเท่านั้น

(๑.๑.๕) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบ เพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๑.๑.๖) ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยเครื่องคอมพิวเตอร์

(๑.๑.๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองใช้งานเมื่อใช้งานเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๒ ชั่วโมง

(๑.๑.๘) ทำการล็อคหน้าจอเครื่องคอมพิวเตอร์หลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานเครื่องคอมพิวเตอร์

(๑.๑.๙) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของสำนักงาน ยกเว้นจะได้รับการตรวจสอบจากฝ่ายสารสนเทศก่อนการใช้งาน

(๑.๒) <u>แนวทางปฏิบัติการใช้รหัสผ่าน</u>

ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ได้กำหนดไว้

(๑.๓) การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(๑.๓.๑) ผู้ใช้ต้องตรวจสอบหาไวรัสจากสื่อต่างๆ ได้แก่ Hard Disk, Thumb Drive และ Data Storge อื่นๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๑.๓.๒) ผู้ใช้ต้องตรวจสอบไฟล์ที่แนบมากับไปรษณีย์อิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

(๑.๓.๓) ผู้ใช้ควรตรวจสอบข้อมูลคอมพิวเตอร์ที่มีชุดคำสั่งไม่พึงประสงค์ ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนด

(๑.๔) การสำรองข้อมูลและการกู้คืน

(๑.๔.๑) ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ ได้แก่ CD, DVD, External Hard Disk เป็นต้น

(๑.๔.๒) ผู้ใช้มีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๒) การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Use of Notebook computer) และอุปกรณ์สื่อสารเคลื่อนที่

(๒.๑) แนวทางปฏิบัติการใช้งานทั่วไป

(๒.๑.๑) เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ที่สำนักงานอนุญาตให้ผู้ใช้ใช้งานเป็นสินทรัพย์ของสำนักงาน ดังนั้น ผู้ใช้ต้องใช้งานเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่อย่างมีประสิทธิภาพเพื่องานของสำนักงาน

(๒.๑.๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ของสำนักงาน ต้องเป็นโปรแกรมที่ได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๒.๑.๓) ผู้ใช้ต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๒.๑.๔) ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

(๒.๑.๕) ในกรณีต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน การตกจากโต๊ะทำงาน หรือหลุดมือ

(๒.๑.๖) หลีกเลี่ยงการใช้นิ้ว หรือของแข็ง หรือปลายปากกา นำไปสัมผัสหน้าจอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ของสำนักงาน ซึ่งอาจทำให้แตกเสียหายได้

(๒.๑.๗) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๒.๑.๘) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุด และต้องเช็ดไปในแนวทางเดียวกันห้ามเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๒.๑.๙) หากมีการนำเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ ซึ่งไม่ใช่สินทรัพย์ของสำนักงานมาใช้กับระบบเครือข่ายของสำนักงาน ต้องได้รับอนุญาตจากฝ่ายสารสนเทศก่อนใช้งาน

(๒.๒) ความปลอดภัยทางด้านกายภาพ

(๒.๑) ผู้ใช้มีหน้าที่รับผิดชอบในการป้องดกันการสูญหาย โดยจะต้องล็อคเครื่องขณะที่ไม่ได้ใช้งาน และไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒.๒) ผู้ใช้ต้องไม่เก็บ หรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน ความชื้น หรือฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

(๒.๓) แนวทางปฏิบัติการใช้รหัสผ่าน

ให้ผู้ใช้ปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ได้กำหนดไว้

(๒.๔) การสำรองข้อมูลและการกู้คืน

(๒.๔.๑) ผู้ใช้ต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์พกพาและอุปกรณ์สื่อสารเคลื่อนที่ของสำนักงาน โดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

(๒.๔.๒) ผู้ใช้จะต้องเก็บรักษาสื่อสำรองข้อมูล Backup Media) ไว้ ในสถานที่ที่เหมาะสม ไม่มีความเสี่ยงต่อการรั่วไหลของข้อมูล

(๒.๔.๓) แผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

(๒.๔.๔) แผ่นสื่อสำรองที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

๗) การควบคุมการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ฝ่ายสารสนเทศ กำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ ภายในสำนักงาน เพื่อดูแลรักษาความมั่นคงปลอดภัยของระบบจากภายนอก มีข้อปฏิบัติ ดังนี้

(๑) ต้องกำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติ เพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกสำนักงาน

(๒) การควบคุมระยะไกล (Remote Desktop) สู่ระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของสำนักงาน การควบคุมบุคคลที่เข้าสู่ระบบของสำนักงานจากระยไกล ต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภาใน

(๓) วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกล ต้องได้รับการอนุมัติจาก CIO หรือผู้ได้รับมอบหมายก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่และข้อมูลอย่างเคร่งครัด

(๔) ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสำนักงานอย่างเพียงพอ และต้องได้รับการอนุมัติจากสำนักงาน

(๕) มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องเหมาะสมแล้วเท่านั้น

(๖) การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานขอความจำเป็นเท่านั้น และไม่เปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอเท่าที่จำเป็นเท่านั้น

๑๑. การบริหารจัดการการบันทึกและตรวจสอบ

๑) กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งานงาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก ได้แก่ บันทึกการ เข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน command line และ firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้ อย่างน้อย ๓ เดือน

๒) มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานงานอย่างสม่ำเสมอ

๓) มีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑๒. การดูแลสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

๑) มีการกำหนดมาตรการป้องกันสินทรพัย์ของสำนักงาน และควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่างๆ ดังนี้

(๑) <u>การจัดการบริเวณล้อมรอบ</u> (Physical Security Management)

(๑.๑) กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน

(๑.๒) พื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ในภายใน (Data Center) ให้ติดตั้งสัญญาณเตือนภัย เพื่อแจ้งเตือนเมื่อมีการบุกรุกเกิดขึ้น

(๑.๔) ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพ เพื่อตรวจสอบว่ายังใช้ได้ตามปกติ

(๑.๕) บุคลากรของสำนักงานต้องล็อค และปิดประตูหน้าต่างอยู่เสมอ หากไม่มีผู้ดูแลเพื่อป้องกันสินทรัพย์ของสำนักงาน

(๒) <u>การควบคุมการเข้า-ออก</u> (Physical Entry Controls)

(๒.๑) ให้มีการบันทึกวันและเวลาเข้า – ออก พื้นที่สำคัญของผู้มาเยือน (Visitors)

(๒.๒) ดูแลผู้ที่มาเยือนในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๒.๓) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญ

(๒.๔) บุคคลภายนอกต้องแจ้งเหตุผลที่เพียงพอในการเข้าถึงบริเวณที่มีความสำคัญ

(๒.๕) สร้างความตระหนักให้ผู้มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์ หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๒.๖) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลอยู่

(๒.๗) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

(๒.๘) มีการพิสูจน์ตัวตน โดยการใช้บัตรรูด และ/หรือ สแกนนิ้ว และ/หรือ การใช้รหัสผ่าน เพื่อควบคุมการเข้า – ออก ในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

(๒.๙) จัดเก็บบันทึกการเข้า – ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center) เพื่อใช้ในการตรวจสอบภายหลังเมื่อมีความจำเป็น

(๒.๑๐) เจ้าหน้าที่ของบริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นชัดเจนตลอดระยะเวลาการปฏิบัติงาน

(๒.๑๑) ผู้ที่มาเยือนต้องติดบัตรให้เห็นชัดเจนตลอดระยะเวลาที่อยู่ในห้องปฏิบัติการ (Server Room)

(๒.๑๒) ต้องจัดให้มีการดูแลและเป้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(๒.๑๓) จัดให้มีการทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบรเวณที่มีความสำคัญอย่างสม่ำเสมอ

(๓) การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภานอก (Public Access, Delivery and Loading Areas)

(๓.๑) จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๓.๒) จำกัดบุคลากร ซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

(๓.๓) จัดพื้นที่หรือบริเวณที่ส่งมอบไว้ เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในสำนักงาน

(๓.๔) ให้ตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะเคลื่อนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

(๓.๕) ลงทะเบียน ตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอก

(๔) การจัดวางและการป้องกันอุปกรณ์ (Equipment Setting and Protection)

(๔.๑) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ในห้อง Data Center ให้น้อยที่สุด

(๔.๒) อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย

(๔.๓) ไม่ให้มการนำอาหาร เครื่องดื่ม และสูบบุหรี่ภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในห้อง Data Center

(๔.๔) ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว โดยมีการตรวจสอบระดับอุณหภูมิ ความชื้น ว่าอยู่ในระดับปกติหรือไม่

(๕) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๕.๑) มีการสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของสำนักงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบ ได้แก่ ระบบสำรองกระแสไฟฟ้า (UPS) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator) ระบบระบายอากาศ ระบบปรับอากาศ และควบคุมความชื้น เป็นต้น

(๕.๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากความล้มเหลวในการทำงานของระบบ

(๕.๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

(๖) การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ (Cabling Security)

(๖.๑) ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณ เพื่อทำให้เกิดความเสียหาย หรือป้องกันสัตว์ต่างๆ กัดสาย

(๖.๒) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๖.๓) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์ เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

(๖.๔) จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(๖.๕) ตู้ Rack ที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(๗) การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๗.๑) ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่กำหนด

(๗.๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๗.๓) จัดเก็บบันทึกกิจกรรมบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๗.๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปรกรณ์ดังกล่าว

(๗.๕) ควบคุมสอดส่องดูแลการปฏิบัติงานของผู้รับจ้างบำรุงรักษาระบบคอมพิวเตอร์ที่มาทำการบำรุงรักษาอุปกรณ์ภายในสำนักงาน

(๗.๖) ควบคุมการส่งอุปกรณ์ออกไปซ่อมแซมนอกสถานที่ เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๘) การนำสินทรัพย์ออกนอกสำนักงาน (Removal of Property)

(๘.๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือสินทรัพย์ออกนอกสำนักงาน

(๘.๒) บันทึกข้อมูลการนำอุปกรณ์ออกนอกสำนักงาน เพื่อใช้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

(๘.๓) สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม

(๙) การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน (Security of Equipment Off – Premises)

(๙.๑) กำหนดมาตรการความปลอดภัย เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือสินทรัพย์ของสำนักงานออกไปใช้งานข้างนอก

(๙.๒) ไม่ทิ้งอุปกรณ์หรือสินทรัพย์ของสำนักงานไว้ในที่สาธารณะ

(๙.๓) ให้เจ้าหน้าที่ที่มีความรับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์เสมือนเป็นสินทรัพย์ของตนเอง

(๑๐) การทำลายอุปกรณ์หรือกานำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Reuse of Equipment)

(๑๐.๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะทำลายอุปกรณ์ดังกล่าว

(๑๐.๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ
- วัฒนธรรมองค์กร

๓) มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

๔) มีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันสินทรัพย์ของหน่วยงาน
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน

- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้ โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารออกจากเครื่องพิมพ์ทันที เมื่อพิมพ์งานเสร็จ

๕) ในการทำลายข้อมูล และสื่อบันทึกข้อมูลประเภทต่างๆ เพื่อป้องกันข้อมูลรั่วไหล และการนำกลับมาใช้ใหม่ เจ้าของข้อมูลต้องปฏิบัติตามแนวทางการทำลาย ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกาDOD ๕๒๒๐.๓๓-M (ซึ่งมีการเขียนทับข้อมูลเดินเป็นจำนวนหลายรอบ)

๑๓. การควบคุมการเข้าใช้งานระบบจากภายนอกศูนย์สารสนเทศ

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในองค์กร เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติดังนี้

๑) การเข้าสู่ระบบระยะไกล (Remote access) สู่ระบบเครือข่ายขององค์กร ต้องควบคุมบุคคลที่จะเข้าสู่ระบบขององค์กรจากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๒) วิธีการใดๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับการอนุมัติจากผู้ดูแลระบบก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของ สพพ. ในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๓) การให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับองค์กรอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอานาจอย่างเป็นทางการ

๔) มีการควบคุม Port ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๕) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๑๔. การพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอก

๑) ผู้ใช้งานระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบขององค์กร ดังนี้

(๑.๑) แสดงชื่อผู้ใช้งานงาน (Username)

(๑.๒) ใส่รหัสผ่าน (Password)

๑๕. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือลักลอบ ทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีข้อปฏิบัติ ดังนี้

๑) การใช้งานรหัสผ่าน (Password Use) และการเปลี่ยนรหัสผ่าน (Change Password)

กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๑) ผู้ใช้งานต้องเก็บรักษารหัสปผ่านไว้ในที่ปลอดภัย ถือเป็นความลับ

(๒) หลีกเลี่ยงการบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือบันทึกลงในกระดาษ หรือในแฟ้มข้อมูล หรือในอุปกรณ์พกพาต่างๆ นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัย และวิธีการในการบันทึกได้รับการอนุมัติแล้ว

(๓) ไม่เก็บรหัสผ่านไว้ในโปรแกรมหรือกระบวนการ Login อัตโนมัติ หรือโปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password)

(๔) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่น ผ่านระบบเครือข่ายคอมพิวเตอร์

(๕) ไม่ใช้รหัสผ่านเดียวกันในกรณีปฏิบัติงานและใช้ส่วนตัว

(๖) ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องจดจำรหัสผ่านหลายตัว ควรใรหัสผ่านเดียวกันที่มีคุณภาพ สำหรับการเข้าถึงทุกระบบ ซึ่งระบบเหล่านั้นต้องมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

(๗) ในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสเนทศ ให้ผู้ใช้งานออกจากระบบ (Log Off) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบเทคโนโลยีสารสนเทศต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหล ต้องเปลี่ยนรหัสผ่านทันที

(๘) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๙) เมื่อเจ้าหน้าที่ของสำนัก/ฝ่าย ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่ขอสิทธิ์การใช้งาน ให้สำนัก/ฝ่าย แจ้งฝ่ายเทคโนโลยีสารสนเทศทันที เพื่อดำเนินการเปลี่ยนสิทธิ์หรือถอดถอนสิทธิ์ของผู้ที่ลาออก จากระบบทันทีที่ได้รับแจ้ง

(๑๐) เปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้ที่ได้สิทธิ์พิเศษ ต้องได้รับการเปลี่ยนเปลงบ่อยกว่าปกติ) และหลีกเลี่ยงการเวียนใช้รหัสผ่านเดิมที่เคยใช้แล้ว

(๑๑) กำหนดให้เปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

(๑๒) เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๑๓) แนวทางการสร้างรหัสผ่านที่มีคุณภาพ

(๑๓.๑) กำหนดรหัสผ่านที่ง่ายต่อการจดจำเฉพาะตน แต่ต้องไม่อยู่บนพื้นฐานของสิ่งที่คนอื่นสามารถคาดเดาได้ง่าย ได้แก่ ชื่อ-นามสกุล หมายเลขโทรศัพท์ และวันเกิด เป็นต้น หรือชื่อ-นามสกุลของบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน

(๑๓.๒) รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร (โดยมีการประสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

(๑๓.๓) รหัสผ่านต้องไม่มีคำซ้ำหรือตัวอักษรซ้ำ ต้องไม่เป็นตัวเลขทั้งหมด หรือตัวอักษรทั้งหมด

(๑๓.๔) ไม่กำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน ได้แก่ ชื่อสกุล วัน เดือน ปีเกิด หรือที่อยู่ เป็นต้น

(๑๓.๕) ไม่กำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

(๑๔) กรณีการแอบอ้างรหัสผ่านหรือนำรหัสผ่านไปใช้โดยไม่ได้รับอนุญาตให้ผู้ใช้งานรีบดำเนินการแจ้งให้ฝ่ายเทคโนโลยีสารสนเทศทราบโดยทันที เพื่อระงับการใช้รหัสผ่านดังกล่าว หรือมีปัญหาการใช้งาน กรณีลืมชื่อผู้ใช้หรือรหัสผ่าน ให้ติดต่อผู้ดูแลระบบ

(๑๕) ผู้ใช้ต้องพึงระลึกเสมอว่า ความมั่นคงปลอดภัยด้านข้อมูลสารสนเทศของสำนักงานที่ตนเองรับผิดชอบอยู่นั้น มีความสำคัญต่อตนและสำนักงานเป็นอย่างยิ่ง ต้องไม่ให้ผู้อื่นบุกรุก แอบอ้าง หรือนำไปใช้ในทางที่ผิด เพราะอาจก่อให้เกิดผลเสียหายเป็นวงกว้างต่องานของตนเองและของสำนักงาน

ส่วนที่ ๔
การควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
(Third party access control)

วัตถุประสงค์

การใช้บริการจากหน่วยงานภายนอก อาจก่อให้เกิดความเสี่ยงได้ ได้แก่ ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารขององค์กร ให้เป็นไปอย่างมั่นคงปลอดภัย และแนวทางในการคัดเลือก ควบคุมการปฏิบัติงานของหน่วยงานภายนอก ได้แก่ การพัฒนาระบบ การใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

แนวทางปฏิบัติ

๑) CIO ต้องดำเนินการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารหรืออุปกรณ์ที่ใช้ในการประมวลผล โดยบุคคลภายในหรือบุคคลภายนอกที่มีความเชี่ยวชาญ รวมถึงกำหนดแผนและมาตรการรองรับหรือแนวทางการแก้ไขที่เหมาะสม

๒) การควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก

(๑.๑) บุคคลภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของ องค์กรจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจาก CIO ก่อน

(๑.๒) จัดทำเอกสารแบบฟอร์มสำหรับให้หน่วยงานภายนอกทำการระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

(๑.๒.๑) เหตุผลในการขอใช้

(๑.๒.๒) ระยะเวลาในการใช้

(๑.๒.๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(๑.๒.๔) การตรวจสอบ MAC address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

(๑.๒.๕) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๓) หน่วยงานภายนอก ที่ทำงานให้กับ สพพ. ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร โดยจะต้องจัดทำสัญญาให้แล้วเสร็จ ก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

๔) หน่วยงานภายนอกที่รับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูล ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนาม ในสัญญาไม่เปิดเผยข้อมูล รวมถึงต้องควบคุมการปฏิบัติงานให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๕) หน่วยงานภายนอกต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอ เพื่อควบคุมหรือตรวจสอบการให้บริการของหน่วยงานภายนอกได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

ส่วนที่ ๕
การใช้งานอินเทอร์เน็ต
(Use of the Internet)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ได้แก่ การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของ สพพ. ถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

๑) ผู้ดูแลระบบ ควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่ สพพ. จัดสรรไว้เท่านั้น ได้แก่ Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่นๆ ยกเว้นมีเหตุผลความจำเป็นและทำการขออนุญาตจาก CIO เป็นลายลักษณ์อักษร

๒) เครื่องคอมพิวเตอร์ส่วนบุคคล ก่อนทำการเชื่อมต่ออินเทอร์เน็ต ผ่านเว็บเบราเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการ และเว็บเบราเซอร์

๓) ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการตรวจสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนรับส่งข้อมูลทุกครั้ง

๔) ผู้ใช้งาน ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของ สพพ. เพื่อหาประโยชน์เชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๕) ผู้ใช้งาน จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของ สพพ.

๖) ผู้ใช้งาน ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับ สพพ.

๗) ห้ามผู้ใช้งาน เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของ สพพ. ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๘) ผู้ใช้งาน ไม่นำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๙) ผู้ใช้งาน ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้ จะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑๐) ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๑๑) ผู้ใช้งาน ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ตซึ่งรวมถึง Patch หรือ Fixes ต่างๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๑๒) ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของ สพพ. รวมถึง การทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่นๆ

๑๓) หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการล๊อกเอ้าท์ออกจากระบบ และปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งาน โดยบุคคลอื่น

ส่วนที่ ๖
การใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของ สพพ. ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้งานจะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

๑) ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของ สพพ. ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้ง มีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ ได้แก่ การลาออก เป็นต้น

๒) ผู้ดูแลระบบ ต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งานรายใหม่ และรหัสผ่านสาหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของ สพพ.

๓) รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น ได้แก่ ‘x’ หรือ ‘*’ ในการพิมพ์แต่ละตัวอักษร

๔) ผู้ดูแลระบบ ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานงานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

๕) ผู้ใช้งานไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๖) ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด ได้แก่ ควรเปลี่ยนรหัสผ่านทุก ๓-๖ เดือน

๗) ผู้ใช้งานควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อ สพพ. หรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้ จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของ สพพ.

๘) ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่น เพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของเป็นครั้งคราว และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๙) ผู้ใช้งาน ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของ สพพ. เพื่อการทำงานของ สพพ. เท่านั้น

๑๐) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการล็อกเอ้าท์ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๑๑) ผู้ใช้งานควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทาการเปิดเพื่อทำการตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File ได้แก่ .exe .com เป็นต้น

๑๒) ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๓) ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม และข้อมูลอันอาจทำให้เสียชื่อเสียงของ สพพ. ทำให้เกิดความแตกแยกระหว่างหน่วยงาน ผ่านทางจดหมายอิเล็กทรอนิกส์

๑๔) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสาคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๑๕) ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๑๖) ผู้ใช้งานควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ส่วนที่ ๗
การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control)

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของ สพพ. โดยการกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

๑. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของ สพพ. จะต้องทำการลงทะเบียน และต้องได้รับการพิจารณาอนุญาตจากผู้ดูแลระบบเป็นลายลักษณ์อักษร

๒. ผู้ดูแลระบบ ต้องทำการลงทะเบียนกาหนดสิทธิ์ผู้ใช้งานงานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓. ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๔. ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตี สามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

๕. ผู้ดูแลระบบควรเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่า สัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้ การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

๖. ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (default) มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

๗. ผู้ดูแลระบบ ควรเปลี่ยนค่า ชื่อล็อกอินและรหัสผ่านสาหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบ ควรเลือกใช้ชื่อล็อกอินและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตี ไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๘. ผู้ดูแลระบบต้องกำหนดค่าใช้ WEB หรือ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

๙. ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC address และชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address และชื่อผู้ใช้งานรหัสผ่าน ตามที่กาหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

๑๐. ผู้ดูแลระบบควรติดตั้งไฟร์วอล (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายใน สพพ.

๑๑. ผู้ดูแลระบบควรให้ผู้ใช้งานในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

๑๒. ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

ส่วนที่ ๘
ระบบรักษาความปลอดภัย
(Security)

ฝ่ายสารสนเทศ ได้มีการวางมาตรการรักษาความปลอดภัยโดยกำหนดอำนาจหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง ในการวางระบบรักษาความปลอดภัย (Security) และระบบการบริหารความเสี่ยงของระบบสารสนเทศ เพื่อเตรียมพร้อมในการแก้ไขปัญหาที่เกิดจากภัยพิบัติได้อย่างรวดเร็วและต่อเนื่องอย่างมีประสิทธิภาพ โดย สพพ. ได้ดำเนินการจัดแบ่งหน้าที่ และบุคลากรผู้รับผิดชอบในการดำเนินงาน ดังนี้

การจัดองค์กรปฏิบัติการฉุกเฉิน หรือสายการบังคับบัญชา (Lines of Authority) เมื่อเกิดเหตุฉุกเฉิน

๑. ผู้อำนวยการ สพพ.

๑) กำหนดนโยบายให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) และ ฝ่ายสารสนเทศ

๒) ให้คำปรึกษาแก่เจ้าหน้าที่สารสนเทศ ในฐานะประธานฝ่ายฯ

๒. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

๑) เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

๒) มีอำนาจสั่งการให้ทุกหน่วยหยุดปฏิบัติการและระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

๓) ทำหน้าที่แทนผู้อานวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมาย หรือขณะที่ผู้อำนวยการระงับเหตุฉุกเฉินไม่อยู่

๔) ประชุมร่วมกับคณะกรรมการจัดการระบบเครือข่ายคอมพิวเตอร์ และคณะกรรมการอื่นที่เกี่ยวข้อง

๕) ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

๖) รายงานข้อมูลและผลการปฏิบัติงานให้ ผู้บริหารระดับสูง ทราบ

๓. ผู้ประสานงานและบริหารการกับดูแลสภาพความพร้อมของระบบเครือข่าย (เจ้าหน้าที่สารสนเทศ)

๑) วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อ CIO

๒) มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉิน จนกว่าผู้อำนวยการระงับเหตุฉุกเฉิน จะมาถึงที่เกิดเหตุ

๓) ประสานงานกับหน่วยงานที่เกี่ยวข้อง ได้แก่ ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง เป็นต้น

๔) รายงานให้ผู้อำนวยการทราบถึงสถานการณ์ และให้สั่งการแนวทางการระงับเหตุฉุกเฉิน

๕) ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

๔. ผู้ดูแลระบบเครือข่ายและผู้ช่วยดูแลระบบเครือข่าย (LAN Administrator and Staffs)

๑) กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

๒) พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่นๆ

๓) ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

๔) ป้องกันชีวิต ทรัพย์สิน และสิ่งแวดล้อม ให้ได้รับความเสียหายน้อยที่สุด

๕) หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุอุปกรณ์ที่ชำรุดเสียหาย แล้วรายงานให้ **CIO** ทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

- ทำการตรวจสอบระบบ Firewall
- ทำการตรวจสอบ Virus, Worm, Spy Ware
- ทำการตรวจสอบ UPS
- ทำการตรวจสอบ Transaction Log Files
- ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่างๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบค่า Configuration ของระบบ

๖) เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้อง เพื่อดำเนินการกู้ระบบโดยเร็ว

๗) ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกในการกู้ระบบ

๘) ทำการสำรองข้อมูลทุกวัน ทุกสัปดาห์ วันศุกร์ทำการสำรองข้อมูลในส่วนของข้อมูล (Data) วันศุกร์สุดท้ายของเดือน ทำการสำรองข้อมูลทั้งระบบ

๙) ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ ได้แก่ โปรแกรมและแฟ้มข้อมูล, รายชื่อโปรแกรม, เอกสารที่เกี่ยวกับระบบปฏิบัติการและโปรแกรม, รายการฮาร์ดแวร์สำรอง, สำเนาคู่มือ

๑๐) นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

๕. ที่ปรึกษาด้านเทคนิค (บุคคลภายนอก)

๑) ให้คำปรึกษาในเรื่องเกี่ยวกับระบบสารสนเทศ และวิธีการจัดการในการระงับเหตุฉุกเฉินที่ปลอดภัยต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อมมากที่สุด

๒) ติดต่อขอคำปรึกษาด้านเทคนิคจากผู้เชี่ยวชาญหรือหน่วยราชการที่เกี่ยวข้อง

๓) ให้คำปรึกษาวิธีการกู้ระบบสารสนเทศกลับคืนมาโดยเร็ว หลังจากเหตุฉุกเฉินสงบแล้ว

ส่วนที่ ๙
การจัดทำระบบสำรองสำหรับระบบเทคโนโลยีสารสนเทศ

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

๑. การคัดเลือกและจัดทำระบบสำรองสำหรับระบบเทคโนโลยีสารสนเทศ

ระบบเทคโนโลยีสารสนเทศที่สำคัญที่ได้พิจารณาคัดเลือกจัดทำระบบสำรอง ได้แก่ ๑) ระบบงาน E-Office ประกอบด้วย ระบบสารบรรณอิเล็กทรอนิกส์ ระบบจองทรัพยากร ระบบเบิกวัสดุอุปกรณ์ ๒) ระบบงาน Back Office ประกอบด้วย ๓) ระบบอินทราเน็ต ๔) ระบบเว็บไซต์ของสำนักงาน ๕) ระบบบริหารเงินทุน ๖) ระบบจัดเก็บเอกสารอิเล็กทรอนิกส์ และ ๗) ระบบบัญชีและการเงิน โดยนำข้อมูลไปเก็บสำรองไว้ที่ศูนย์สำรองข้อมูล (DR Site) ตามวิธีการและข้อปฏิบัติของ สพพ.

สำหรับระบบเทคโนโลยีสารสนเทศอื่นที่ไม่ได้จัดเก็บสำรองไว้ที่ศูนย์สำรองข้อมูล (DR Site) ของ สพพ. หากมีความจำเป็นต้องการทำการสำรองข้อมูลเก็บไว้ มีข้อปฏิบัติ ดังนี้

๑) กำหนดรายละเอียดของระบบงานที่มีความจำเป็นต้องสำรองข้อมูลเก็บไว้ ประกอบด้วยข้อมูลในระบบ ข้อมูลของระบบงาน และข้อมูลสำหรับตัวระบบ ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการและซอฟต์แวร์อื่นๆ ที่เกี่ยวข้อง เป็นต้น

๒) ขั้นตอนการจัดทำสำรองข้อมูล และการกู้คืนข้อมูลอย่างถูกต้อง

๓) กำหนดวิธีการสำรองแบบ Full Backup หรือ Incremental Backup ที่เหมาะสมกับระบบงาน โดยคำนึงถึงความสำคัญของระบบงานและข้อมูลสารสนเทศของระบบงานนั้น

๔) เตรียมอุปกรณ์ที่จำเป็นต่อการสำรองข้อมูล และการกู้คืนข้อมูล

๕) ทำการสำรองข้อมูลตามชนิด ความถี่ และวิธีการสำรองที่ได้กำหนดไว้ และให้ตรวจสอบอย่างสม่ำเสมอว่าข้อมูลสำรองไว้นั้นมีความครบถ้วน

๖) ต้องนำข้อมูลที่สำรองไปเก็บไว้นอกสถานที่อย่างน้อย ๑ ชุด

๒. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน

๑) ระบุวัตถุประสงค์หลักของแผนเตรียมความพร้อมกรณีฉุกเฉิน

๒) จัดทำบัญชีรายชื่อของระบบงานที่มีความสำคัญ รวมทั้งปรับปรุงบัญชีรายชื่อดังกล่าวให้มีความทันสมัยอยู่เสมอ

๓) กำหนดปัจจัยเสี่ยงและภัยพิบัติที่อาจส่งผลกระทบกับระบบงานที่สำคัญ และกำหนดมาตรการเพื่อลดความเสี่ยงที่พบในกรณีต่างๆ ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๔) ประเมินสถานการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๕) จัดทำแผนกู้คืนเพื่อรับมือกับสถานการณ์ความเสี่ยงที่อาจเกิดขึ้นได้ โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

(๑) กำหนดหน้าที่ความรับผิดชอบต่อผู้ที่เกี่ยวข้องทั้งหมด

(๒) ขั้นตอนปฏิบัติในการกู้คืนระบบงาน โดยมีแนวทางและข้อปฏิบัติตามแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

(๓) การกำหนดช่องทางในการติดต่อผู้ให้บริการภายนอก หรือผู้ให้บริการเครือข่ายฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) เมื่อเกิดเหตุจำเป็นต้องติดต่อ

๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๗) ให้ทำการปรับปรุงแผนกู้คืนอย่าน้อยปีละ ๑ ครั้ง

๘) ให้จัดประชุมและแจ้งให้ผู้เกี่ยวข้องทั้งหมดได้รับทราบรายละเอียดของแผนกู้คืน รวมทั้งเมื่อมีการปรับปรุงแผนกู้คืนใหม่จะต้องจัดประชุมใหม่ และแจ้งให้ผู้ที่เกี่ยวข้องทราบเช่นเดียวกัน

๓. การกำหนดหน้าที่และความรับผิดชอบของบุคลากร

กำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบเทคโนโลยีสารสนเทศระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ระบุไว้ในแผนบริหารความเสี่ยงเพื่อความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศและแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน (IT Contingency Plan) แผนสำรองข้อมูลและระบบเทคโนโลยีสารสนเทศ

๔. การทดสอบสภาพพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ ระบบสำรองและระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน

ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ โดยดำเนินการ ดังนี้

๑) ฝ่ายสารสนเทศได้เตรียมศูนย์คอมพิวเตอร์สำรอง (DR-Site) เพื่อเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบงานตามลำดับความสำคัญคืนมาให้ใช้งานได้ภายในระยะเวลาที่เหมาะสม โดยมีการทดสอบปีละ ๑ ครั้ง

๒) มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๕. ระยะความถี่ของการปฏิบัติ

๑) ระยะความถี่การสำรองข้อมูลของระบบงาน ขึ้นอยู่กับความสำคัญของระบบ และสภาพเปลี่ยนแปลงของระบบงานนั้นๆ โดยระบบงานที่มีการเปลี่ยนแปลงบ่อย ต้องมีความถี่ในการสำรองข้อมูลมากขึ้น

๒) ทำการทดสอบกู้คืนข้อมูลที่สำรองไว้ และความพร้อมในการใช้งาน อย่างน้อยปีละ ๑ ครั้ง

๓) ให้ปรับปรุงรายงานการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๑๐
การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑. วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

๒. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๑) ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของ สพพ. เพื่อการตรวจสอบและประเมินความเสี่ยงนั้น ดังต่อไปนี้

(๑) ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

(๒) ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สาย โดยไม่ได้รับอนุญาต

(๓) ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

(๔) ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) ระบบสารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกันมากกว่าหนึ่งจุด

(๕) ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่น โดยไม่ได้รับอนุญาต

(๖) จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

(๗) มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๒) กำหนดวิธีการในการตรวจสอบและประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๓) การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ ดังต่อไปนี้

(๑) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

(๒) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

(๓) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

(๔) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายใน สพพ. เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ ความเสียหายหรืออันตรายที่จะเกิดขึ้นของหน่วยงาน

ส่วนที่ ๑๑
การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๑. วัตถุประสงค์

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๒. การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑) จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของ สพพ.

๒) จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

๓) ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อระวัง ใ.นรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

๔) ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ส่วนที่ ๑๒
การกำหนดหน้าที่ผู้รับผิดชอบของผู้ใช้งาน
(User Responsibilities)

กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. หน้าที่ความรับผิดชอบแยกตามตำแหน่งงานที่เกี่ยวข้อง ดังนี้

๑. ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO)

๑) กำกับให้มีการกำหนดจัดทำปรับปรุงนโยบายความมั่นคงปลอดภัยอยู่เสมอ

๒) กำกับให้มีการควบคุม และปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด ห้ามมิให้ ผู้ใดฝ่าฝืน หรือละเลยการปฏิบัติตามแนวทางนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓) มอบหมายอำนาจหน้าที่ให้ผู้ดูแลควบคุม และถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด

๒. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

๑) เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

๒) มีอำนาจสั่งการให้ทุกหน่วยหยุดปฏิบัติการและระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ

๓) ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมาย หรือขณะที่ ผู้อำนวยการระงับเหตุฉุกเฉินไม่อยู่

๔) ประชุมร่วมกับคณะกรรมการจัดการระบบเครือข่ายคอมพิวเตอร์ และคณะกรรมการอื่นที่เกี่ยวข้อง

๕) ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

๖) รายงานข้อมูลและผลการปฏิบัติงานให้ ผู้บริหารระดับสูง ทราบ

๓. ผู้ประสานงานและบริหารการกับดูแลสภาพความพร้อมของระบบเครือข่าย (เจ้าหน้าที่สารสนเทศ)

๑) วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อ CIO

๒) มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉิน จนกว่าผู้อำนวยการระงับเหตุฉุกเฉินจะมาถึงที่เกิดเหตุ

๓) ประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง เป็นต้น

๔) รายงานให้ผู้อำนวยการทราบถึงสถานการณ์ และให้สั่งการแนวทางการระงับเหตุฉุกเฉิน

๕) ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

๔. ผู้ดูแลระบบเครือข่าย และผู้ช่วยดูแลระบบเครือข่าย (LAN Administrator and Staffs)

๑) กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

๒) พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่นๆ

๓) ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

๔) ป้องกันชีวิต ทรัพย์สิน และสิ่งแวดล้อม ให้ได้รับความเสียหายน้อยที่สุด

๕) หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุ อุปกรณ์ที่ชำรุดเสียหาย แล้วรายงานให้ CIO ทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

- ทำการตรวจสอบระบบ firewall
- ทำการตรวจสอบ Virus, Worm, Spy ware
- ทำการตรวจสอบ UPS
- ทำการตรวจสอบ Transaction log files
- ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่างๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบค่า Configuration ของระบบ

๖) เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ software ตลอดจนอุปกรณ์ที่เกี่ยวข้อง เพื่อดำเนินการกู้ระบบโดยเร็ว

๗) ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกในการกู้ระบบ

๘) ทำการสำรองข้อมูลทุกสัปดาห์ วันศุกร์ทำการสำรองข้อมูลในส่วนของข้อมูล (Data) วันศุกร์สุดท้ายของเดือน ทำการสำรองข้อมูลทั้งระบบ

๙) ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ เช่น โปรแกรมและแฟ้มข้อมูล, รายชื่อโปรแกรม, เอกสารที่เกี่ยวกับระบบปฏิบัติการและโปรแกรม, รายการฮาร์ดแวร์สำรอง, สำเนาคู่มือ

๑๐) นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

๕. ที่ปรึกษาด้านเทคนิค (บุคคลภายนอก)

๑) ให้คำปรึกษาในเรื่องเกี่ยวกับระบบสารสนเทศ และวิธีการจัดการในการระงับเหตุฉุกเฉินที่ปลอดภัยต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อมมากที่สุด

๒) ติดต่อขอคำปรึกษาด้านเทคนิคจากผู้เชี่ยวชาญหรือหน่วยราชการที่เกี่ยวข้อง

๓) ให้คำปรึกษาวิธีการกู้ระบบสารสนเทศกลับคืนมาโดยเร็ว หลังจากเหตุฉุกเฉินสงบแล้ว

๖. หัวหน้าหน่วยงานที่เกิดเหตุ (On-site manager)

๑) แจ้งเหตุฉุกเฉิน และเคลื่อนย้ายตนเอง และผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

๒) ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ประธานศูนย์ประสานงานรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

๓) นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพ และสอบทานบัญชีทรัพย์สินที่จัดทำขึ้นมา และทำรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

๒. ระดับนโยบาย

ให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานที่ทำหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) และผู้อำนวยการสำนัก เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน) ติดตาม และกำกับดูแล ควบคุมตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติ

๔. แนวทางปฏิบัติของผู้รับผิดชอบ

๑. CIO/ผู้ที่ได้รับมอบหมาย รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงาน อย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการ ปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการ รวมทั้งรับผิดชอบ ดังนี้

๑.๑) ควบคุมการเข้า - ออกห้อง Server ตามการกำหนดสิทธิ์การเข้าถึง Server

๑.๒) กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดให้ สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม.

๑.๓) กำกับดูแล การติดตั้ง รื้อถอน ดูแล ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN, Internet, Intranet ที่ให้บริการใน สพพ.

๑.๔) กำกับดูแลรักษาการทำงานระบบดับเพลิงอัตโนมัติของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ให้สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้

๑.๕) แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

๑.๖) รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาระดับสูงทราบสม่ำเสมอ

๑.๗) กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตามสิทธิ์การเข้าถึงระบบ

๑.๘) กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาตตามแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศเพื่อนบ้าน (องค์การมหาชน)

๑.๙) กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ใน Server ของระบบฐานข้อมูลทั้งหมดที่ให้บริการในเว็บไซต์ ให้สามารถใช้ งานได้ตามปกติตลอด ๒๔ ชม.

๑.๑๐) กำกับดูแล ตรวจสอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบอื่น

แผนผังสายการบังคับบัญชา (Lines of Authority)

ภาคผนวก

ระบบรักษาความปลอดภัย (Security)

ระบบรักษาความปลอดภัย (Security)

ฝ่ายสารสนเทศ สพพ. ได้มีการวางมาตรการรักษาความปลอดภัยโดยกำหนดอำนาจหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้อง ในการวางระบบรักษาความปลอดภัย (Security) และระบบการบริหารความเสี่ยงของระบบสารสนเทศ เพื่อเตรียมพร้อมในการแก้ไขปัญหาที่เกิดจากภัยพิบัติได้อย่างรวดเร็วและต่อเนื่องอย่างมีประสิทธิภาพ โดย สพพ. ได้ดำเนินการจัดแบ่งหน้าที่ และบุคลากรผู้รับผิดชอบในการดำเนินงาน ดังนี้

การจัดองค์กรปฏิบัติการฉุกเฉิน หรือสายการบังคับบัญชา (Lines of Authority) เมื่อเกิดเหตุฉุกเฉิน

๑. ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO)

๑) กำหนดนโยบายให้ CIO และ ฝ่ายสารสนเทศ

๒) ให้คำปรึกษาแก่เจ้าหน้าที่สารสนเทศ ในฐานะประธานศูนย์ฯ

๒. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

๑) เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

๒) มีอำนาจสั่งการให้ทุกหน่วยหยุดปฏิบัติการและระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

๓) ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมาย หรือขณะที่ผู้อำนวยการระงับเหตุฉุกเฉินไม่อยู่

๔) ประชุมร่วมกับคณะกรรมการจัดการระบบเครือข่ายคอมพิวเตอร์ และคณะกรรมการอื่นที่เกี่ยวข้อง

๕) ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯตามความเหมาะสม

๖) รายงานข้อมูลและผลการปฏิบัติงานให้ ผู้บริหารระดับสูง ทราบ

๓. ผู้ประสานงานและบริหารการกับดูแลสภาพความพร้อมของระบบเครือข่าย (เจ้าหน้าที่สารสนเทศ)

๑) วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อ CIO

๒) มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉิน จนกว่าผู้อำนวยการระงับเหตุฉุกเฉิน จะมาถึงที่เกิดเหตุ

๓) ประสานงานกับหน่วยงานที่เกี่ยวข้อง ได้แก่ ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง เป็นต้น

๔) รายงานให้ผู้อำนวยการทราบถึงสถานการณ์ และให้สั่งการแนวทางการระงับเหตุฉุกเฉิน

๕) ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

๔. ผู้ดูแลระบบเครือข่ายและผู้ช่วยดูแลระบบเครือข่าย (LAN Administrator and Staffs)

๑) กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

๒) พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่นๆ

๓) ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

๔) ป้องกันชีวิต ทรัพย์สิน และสิ่งแวดล้อม ให้ได้รับความเสียหายน้อยที่สุด

๕) หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุ อุปกรณ์ที่ชำรุดเสียหาย แล้วรายงานให้ CIO ทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

- ทำการตรวจสอบระบบ firewall
- ทำการตรวจสอบ virus, worm, spy ware
- ทำการตรวจสอบ UPS
- ทำการตรวจสอบ Transaction log files
- ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่างๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบค่า Configuration ของระบบ

๖) เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ software ตลอดจนอุปกรณ์ที่เกี่ยวข้อง เพื่อดำเนินการกู้ระบบโดยเร็ว

๗) ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกในการกู้ระบบ

๘) ทำการสำรองข้อมูลทุกสัปดาห์ วันศุกร์ทำการสำรองข้อมูลในส่วนของข้อมูล (data) วันศุกร์สุดท้ายของเดือน ทำการสำรองข้อมูลทั้งระบบ

๙) ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ ได้แก่ โปรแกรมและแฟ้มข้อมูล, รายชื่อโปรแกรม, เอกสารที่เกี่ยวกับระบบปฏิบัติการและโปรแกรม, รายการฮาร์ดแวร์สำรอง, สำเนาคู่มือ

๑๐) นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

๕. ที่ปรึกษาด้านเทคนิค (บุคคลภายนอก)

๑) ให้คำปรึกษาในเรื่องเกี่ยวกับระบบสารสนเทศ และวิธีการจัดการในการระงับเหตุฉุกเฉินที่ปลอดภัยต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อมมากที่สุด

๒) ติดต่อขอคำปรึกษาด้านเทคนิคจากผู้เชี่ยวชาญหรือหน่วยราชการที่เกี่ยวข้อง

๓) ให้คำปรึกษาวิธีการกู้ระบบสารสนเทศกลับคืนมาโดยเร็ว หลังจากเหตุฉุกเฉินสงบแล้ว

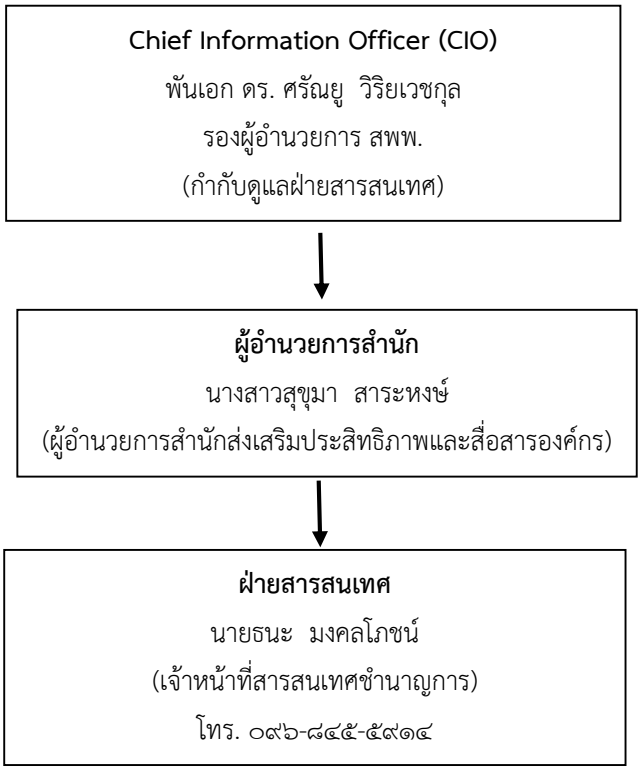
๖. หัวหน้าหน่วยงานที่เกิดเหตุ (On-site manager)

๑) แจ้งเหตุฉุกเฉิน และเคลื่อนย้ายตนเองและผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

๒) ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ประธานศูนย์ประสานงานรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

๓) นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพ และสอบทานบัญชีทรัพย์สินที่จัดทำขึ้นมา และทำรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

แผนผังสายการบังคับบัญชา (Lines of Authority) เมื่อเกิดเหตุฉุกเฉิน



แผนเตรียมความพร้อมกรณีฉุกเฉิน แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ (IT Contingency Plan)

แผนเตรียมความพร้อมกรณีฉุกเฉิน
แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ
(IT Contingency Plan)

๑. หลักการและเหตุผล

ปัจจุบันภัยที่เกิดกับระบบเทคโนโลยีสารสนเทศมีอัตราการเกิดเพิ่มขึ้น ตามความก้าวหน้าของเทคโนโลยีสารสนเทศ ภัยอันตรายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศอาจเกิดขึ้นได้โดยคน ซึ่งได้แก่ เจ้าหน้าที่ บุคลากรของหน่วยงานที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ สถานการณ์ หรือเหตุการณ์ทั้งเจตนาและไม่เจตนา อันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผย หรือเปลี่ยนแปลง ทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่นๆ ตามความสาเหตุของภัย ดังนั้น เพื่อเป็นการลดภัยดังกล่าวที่จะเกิดขึ้นในระบบเทคโนโลยีสารสนเทศของ สพพ. ฝ่ายสารสนเทศ จึงต้องมีการจัดทำแผนรองรับการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

๒. วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมใช้งาน

๒. เพื่อลดความเสียหายที่จะเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบฐานข้อมูลและสารสนเทศ

๓. แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (Contingency Plan)

ข้อควรปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติหรือการใช้งานระบบเครือข่ายขัดข้อง

๓.๑ กรณีเครื่องลูกข่าย

๑) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้เจ้าหน้าที่สารสนเทศทราบ หรือกรณีมีเหตุอันทำให้ ฝ่ายสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ฝ่ายสารสนเทศจะต้องประกาศให้ทุกหน่วยงานใน สพพ. ทราบ

๒) เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว

๓) ปิดระบบไฟฟ้าที่เข้าเครื่องทั้งหมด

๔) ขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๕) ให้เจ้าหน้าที่สารสนเทศ แจ้งเหตุขัดข้องนั้นให้ CIO ทราบโดยเร็วที่สุด

๓.๒ กรณีเครื่องแม่ข่าย (Server) และอุปกรณ์เครือข่าย

๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

๒) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ, ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๓) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๔) รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๕) ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๖) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๗) ผู้ดูแลระบบ ต้องรีบแจ้งให้ CIO ทราบโดยเร็ว

๓.๓ ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

๑) กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

(๑.๑) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ, ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

(๑.๒) ในกรณีไฟไหม้ ให้ตัดระบบจ่ายไฟ ให้ใช้น้ำยาดับเพลิงควบคุมเพลิงโดยเร็ว

(๑.๓) ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลบำรุงรักษาระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

(๑.๔) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำ อุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๒) กรณีเครื่องลูกข่าย

(๒.๑) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้เจ้าหน้าที่สารสนเทศทราบ หรือกรณีมีเหตุอันทำให้ ฝ่ายสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ฝ่ายสารสนเทศจะต้องประกาศให้ทุกหน่วยงานใน สพพ. ทราบ

(๒.๒) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย(สาย LAN) ออกจากเครื่องนั้นโดยเร็ว และแจ้งให้เจ้าหน้าที่ฝ่ายสารสนเทศดำเนินการ

๔. แผนดำเนินการเพื่อให้ระบบใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan)

เพื่อแก้ไขระบบเทคโนโลยีสารสนเทศของ สพพ. ที่เกิดจากภัยพิบัติให้ใช้งานได้อย่างรวดเร็วและต่อเนื่องอย่างมีประสิทธิภาพ สพพ. ได้ดำเนินการจัดแบ่งหน้าที่และบุคลากรผู้รับผิดชอบดำเนินงาน ดังนี้

การจัดองค์กรปฏิบัติการฉุกเฉินในระบบเทคโนโลยีสารสนเทศ สพพ. เมื่อเกิดเหตุฉุกเฉิน

๑. รองผู้อำนวยการ สพพ. (กำกับดูแลฝ่ายสารสนเทศ)

๑) กำหนดนโยบายให้ ฝ่ายสารสนเทศ

๒) ให้คำปรึกษาแก่เจ้าหน้าที่สารสนเทศ ในฐานะประธานศูนย์ฯ

๒. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

๑) เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

๒) มีอำนาจสั่งการให้ทุกหน่วยหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

๓) มีอำนาจสั่งทำลายกุญแจ อาคารเก็บวัตถุอันตรายเพื่อการระงับเหตุฉุกเฉิน

๔) ประชุมร่วมกับคณะกรรมการจัดการระบบเครือข่ายคอมพิวเตอร์ และคณะกรรมการอื่นที่เกี่ยวข้อง

๕) ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

๖) รายงานข้อมูลและผลการปฏิบัติงานให้ ผู้บริหารระดับสูง ทราบ

๓. ผู้ประสานงานและบริหารการกับดูแลสภาพความพร้อมของระบบเครือข่าย (ฝ่ายสารสนเทศ)

๑) วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อ CIO

๒) มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉิน จนกว่าผู้อำนวยการระงับเหตุฉุกเฉิน จะมาถึงที่เกิดเหตุ

๓) การให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ

๔) ทำหน้าที่แทนผู้อานวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมาย หรือขณะที่ ผู้อำนวยการระงับเหตุฉุกเฉินไม่อยู่

๕) ประสานงานกับหน่วยงานที่เกี่ยวข้อง ได้แก่ ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง เป็นต้น

๖) รายงานให้ผู้อำนวยการระงับเหตุฉุกเฉินทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

๗) กำหนดอัตรากำลังพล วัสดุอุปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

๘) ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

๔. ผู้ดูแลระบบเครือข่ายและผู้ช่วยดูแลระบบเครือข่าย (LAN Administrator and Staffs)

๑) กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทาการดับเพลิง

๒) พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่นๆ มาช่วย

๓) ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

๔) ป้องกันชีวิต ทรัพย์สิน และสิ่งแวดล้อม ให้ได้รับความเสียหายน้อยที่สุด

๕) หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำาเนินการตรวจสอบ วัสดุ อุปกรณ์ที่ชำรุดเสียหาย แล้วรายงานให้ CIO ทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

- ทำการตรวจสอบระบบ Firewall
- ทำการตรวจสอบ Virus, Worm, Spy Ware

- ทำการตรวจสอบ UPS
- ทำการตรวจสอบ Transaction Log Files
- ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่างๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบค่า Configuration ของระบบ

๖) เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้อง เพื่อดำเนินการกู้ระบบโดยเร็ว

๗) ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทที่ปรึกษาในการกู้ระบบ

๘) ทำการสำรองข้อมูลทุกสัปดาห์ วันศุกร์ทำการสำรองข้อมูลในส่วนของข้อมูล (Data) วันศุกร์สุดท้ายของเดือน ทำการสำรองข้อมูลทั้งระบบ

๙) ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ ได้แก่ โปรแกรมและแฟ้มข้อมูล, Tape Backup, รายชื่อโปรแกรม, เอกสารที่เกี่ยวกับระบบปฏิบัติการและโปรแกรม, รายการฮาร์ดแวร์สำรอง, สำเนาคู่มือ

๑๐) นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

๕. ที่ปรึกษาด้านเทคนิค (วิศวกรที่ปรึกษา และเจ้าหน้าที่บริษัทที่ปรึกษา)

๑) ให้คำปรึกษาในเรื่องเกี่ยวกับระบบสารสนเทศ และวิธีการจัดการในการระงับเหตุฉุกเฉินที่ปลอดภัยต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อมมากที่สุด

๒) ติดต่อขอคำปรึกษาด้านเทคนิคจากผู้เชี่ยวชาญหรือหน่วยราชการที่เกี่ยวข้อง

๓) ให้คำปรึกษาวิธีการกู้ระบบสารสนเทศกลับคืนมาโดยเร็ว หลังจากเหตุฉุกเฉินสงบแล้ว

๖. หัวหน้าหน่วยงานที่เกิดเหตุ (On-site manager)

๑) แจ้งเหตุฉุกเฉิน และเคลื่อนย้ายตนเองและผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

๒) ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ประธานศูนย์ประสานงานรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

๓) นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพ และสอบทานบัญชีทรัพย์สินที่จัดทำขึ้นมา และทำรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

๕. แผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Procedure) และการกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์เครือข่าย (System Recovery)

ระบบเครื่องแม่ข่ายและอุปกรณ์เครือข่าย โดยปกติจะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการเครื่องลูกข่ายต่างๆ ได้ ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดเท่าที่จะทำได้ เนื่องจากเครื่องแม่ข่ายและอุปกรณ์เครือข่าย ต้องทำงานด้านบริการ (Service) แก่เครื่องลูกข่ายให้สามารถใช้งานได้ปกติ การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์เครือข่าย จำเป็นต้องทำอย่างรวดเร็ว เพื่อให้ใช้งานได้อย่างรวดเร็วที่สุด

แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์ และแฟ้มข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน

๑. ฝ่ายสารสนเทศสำรองข้อมูลและซอฟต์แวร์เก็บไว้บน Cloud เป็นรายวัน รายสัปดาห์ และรายเดือน โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของ สพพ. จากจำเป็นมากไปหาน้อย

๒. ฝ่ายสารสนเทศจัดทำขั้นตอนการปฏิบัติการและจัดทำการสำรองข้อมูล และการกู้คืนข้อมูลอย่างสม่ำเสมอทุกเดือน หรือตามความเหมาะสมไปยังศูนย์กู้คืนระบบจากความเสียหายทางภัยพิบัติ (DR-Site) ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

๓. ฝ่ายสารสนเทศได้จัดเก็บ Cloud ที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้น ให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน และทำการจัดเก็บ CD-ROM / HARDDISK / Flash drive สำรองข้อมูลรายเดือนแยกไว้ ณ สถานที่อื่น

๔. ฝ่ายสารสนเทศได้เตรียมศูนย์คอมพิวเตอร์สำรอง (DR-site) เพื่อเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้สามารถกู้ระบบงานตามลำดับความสำคัญคืนมาให้ใช้งานได้ภายในระยะเวลาที่เหมาะสม โดยมีการทดสอบปีละ ๑ ครั้ง

๕. มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วย วิธีการทางอิเล็กทรอนิกส์เป็นลำดับชั้น โดย CIO เป็นผู้กำกับดูแลการปฏิบัติงาน

๖. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๗. มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์

๘. มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่างๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ

๙. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

แผนการจัดฝึกอบรมด้านเทคโนโลยีสารสนเทศ

แผนงาน/โครงการจัดฝึกอบรมด้านเทคโนโลยีสารสนเทศ ระยะ 5 ปี (พ.ศ. 2560 – 2564)

ลำดับ	ชื่อโครงการ	วัตถุประสงค์	ปีงบประมาณ					เป็นเงินทั้งสิ้น	ผู้รับผิดชอบ	ตัวชี้วัด
			2560	2561	2562	2563	2564			
1	โครงการฝึกอบรม/สัมมนา เพื่อพัฒนาความรู้และเพิ่มทักษะด้าน ICT แก่เจ้าหน้าที่ สพพ.	เพื่อให้พนักงานด้านสารสนเทศ มีความตระหนักและสามารถดูแลป้องกัน วางแผน บริหารจัดการสารสนเทศ ได้อย่างมีประสิทธิภาพ และเพื่อให้เจ้าหน้าที่มีความรู้ตระหนักต่อความสำคัญและกฎหมายต่างๆ ทางด้านสารสนเทศ	290,000	200,000	310,000	200,000	200,000	1,200,000	สำนักอำนวยการ สำนักนโยบายและแผน สำนักบริหารโครงการ สำนักบริหารเงินทุน สำนักความช่วยเหลือทางวิชาการ	1. มีการอบรม ตามหลักสูตรที่กำหนดไว้ในแผน 2. มีผู้ได้รับการอบรมครบถ้วนตามแผน 3. ผู้เข้ารับการฝึกอบรม มีความรู้ความเข้าใจด้านความตระหนักและสามารถดูแลป้องกัน วางแผน บริหารจัดการด้านสารสนเทศมากขึ้น เมื่อเทียบกับก่อนการเข้ารับการฝึกอบรม 4. ผู้เข้ารับการฝึกอบรมได้รับใบรับรองการผ่านการฝึกอบรม
		รวม	**290,000**	**200,000**	**310,000**	**200,000**	**200,000**	**1,200,000**		